On optimising quantum communication in verifiable quantum computing

Theodoros Kapourniotis[1], Vedran Dunjko[1,2,3], and Elham Kashefi[1,4]

[1]*School of Informatics, University of Edinburgh, UK*
[2]*Division of Molecular Biology, Ruder Boskovic Institute, Zagreb, Croatia*
[3]*Now at: Institute for Theoretical Physics, University of Innsbruck, Austria*
[4]*Now at: CNRS, TelecomParis Tech, France*

June 24, 2015

Abstract

In the absence of any efficient classical schemes for verifying a universal quantum computer, the importance of limiting the required quantum resources for this task has been highlighted recently. Currently, most of efficient quantum verification protocols are based on cryptographic techniques where an almost classical verifier executes her desired encrypted quantum computation remotely on an untrusted quantum prover. In this work we present a new protocol for quantum verification by incorporating existing techniques in a non-standard composition to reduce the required quantum communications between the verifier and the prover.

1 Introduction

As quantum technology scales, verifying that a quantum black box device does what it promises becomes a difficult problem [1]. In particular, verification implies that the probability of accepting the output returned by a remote quantum computation and the output being incorrect, can be made arbitrarily small. Providing a solution to this problem is crucial in the context of secure delegated quantum computing where a weak verifier is required to perform a complex computation with the help of an untrusted quantum prover [2–9]. Also, in lab settings, where an experimentalist wants to verify that the state returned by a scalable quantum experiment is correct, standard techniques like quantum tomography become intractable, for few examples see [10–13].

To achieve a practical verification protocol (from the verifier's point of view) one aims to minimise the required resources of the verifier. This means optimising the number of operations that the verifier has to apply as well as reducing the classical and quantum communication rounds between verifier and prover, while limiting the quantum capabilities of the verifier in terms of the states preparation and quantum operations he can apply. Recently several verification protocols have been proposed, each targeting particular aspects of the above optimisation goal [3, 5–8, 14–18].

In this paper we are concerned with two such protocols, one with an optimal state preparation, proposed by Fitzsimons and Kashefi (referred to here as the FK protocol [5]), the other with better communication cost scaling proposed by Aharonov, Ben-Or and Eban (referred to here as the ABE protocol and is the second of the two protocols presented in [6]). In the FK protocol the verifier is required to have the minimal quantum capacity of preparing single random qubits, while due

to the complexity of the underlying resource state necessary for the prover's universal quantum computation, the communication overhead is quadratic in the input size. In contrast, the ABE protocol enjoys a linear overhead in the input size however the cost is the verifier's requirement of preparing highly entangled secretly encoded states which scale with the security parameter. The main contribution of this paper is to show how we can keep the best of the two approaches. In doing so we ought to prove several new properties of these two protocols that could become useful in other context as well.

Our FK-ABE hybrid protocol is based on the blindness property of the FK protocol where the prover does not learn anything about the computation. Hence, the verifier can remotely and securely prepare the entangled encoded state needed for the ABE protocol on the prover side. After this preparation stage is performed via the FK protocol, without obtaining the state back, verifier continues with the steps of the ABE protocol to perform the (public) logical computation and check if the output state is valid. Crucially, as we prove, the techniques of the FK protocol can be used separately for the preparation of each encoded input state of the ABE protocol, avoiding the construction of a global quadratic size resource state used in the original FK protocol. Hence the overall complexity of the hybrid protocol remains linear in the input size while we get the advantage of preparing single qubit states (in this case qudit to match the ABE protocol) as opposed to the highly entangled encoded states required for the original ABE protocol. However, several issues had to be resolved in order to construct the hybrid protocol.

- The verification procedure of the FK protocol involves measuring special *trap* qubits that are placed at random positions including among the output system (the final qubits not measured by prover). In order to keep the verifier as simple as possible, i.e. not requiring any quantum memory capability, unlike the original FK protocol, the final output state prepared at the first stage of the hybrid protocol is not returned to the verifier. However the position of the actual output of the computation should be made public so that prover can apply the public logical circuit of the ABE protocol. This is achieved by adding extra blind computation steps that localise the position of the output without leaking the positions of the traps.

- The final output of the modified localising protocol, as explained above, by construction does not contain any traps. Therefore the prover can replace this state by any state of his choice and there is no mechanism for the verifier to detect his deviation. However, we show that, due to blindness, the output state has the correct structure to be verifiable by the ABE protocol stage of the hybrid protocol and can possibly be used in any other hybrid compositions that involve similar verification techniques.

- The ABE protocol has to be proved to be robust, since due to the above mentioned issues, the output prepared by the FK protocol stage could be deviated from the ideal ABE protocol input. We show that as long as the deviation is independent of any secret parameter of the verifier the ABE protocol succeeds.

- Finally, we also prove that the classical communication between verifier and prover, necessary for executing the logical circuit computation in the ABE protocol, does not leak any information that violates the blindness requirement in the context of the hybrid protocol, thus not affecting the verification property.

1.1 Related work

A different verification approach was proposed in [7] where the verifier is fully classical but the computation is delegated to non-signalling entangled provers and the communication overhead is

huge due to the rigidity requirement for testing CHSH inequalities. While the communication of this protocol has been improved recently [16, 17], also through a hybrid composition with the FK protocol, however the bound achieved there is substantially higher (at least quartic) than the linear bound of the presented protocol. Other work on quantum verification includes [3] where there is a restriction on the permitted set of functions, referred to as random verifiable. In [8] a verification protocol is presented with the focus being on constructing a quantum one time program rather than improving on the practicality of verification. In [18] a verification protocol is given where the prover is able to send quantum states back to the verifier which has the capacity to measure them. Focusing on the blindness property only, several recent papers [19–21] have achieved better than linear bound while compromising either unconditional security property or simplicity of the verifier quantum operation. We believe that it may be worthwhile to explore these new blindness techniques with the goal of designing more efficient verification protocols.

Before formalizing the main results of this paper, we give a short overview of the FK and ABE protocols.

1.2   Overview of the FK and ABE protocols

A security property that is defined in the delegated computing scenario and used as a stepping stone in the construction of the FK protocol is blindness [5]. The verifier (Alice) wants to delegate a computation to the prover (Bob) while hiding both the input and the computation. Bob's possible deviation is not constrained in any way.

Definition 1 (Perfect Blindness)**.** *Let P be a protocol for delegated computation: Alice's input is a description of a computation on a quantum input, which she needs to perform with the aid of Bob and return the correct quantum output. Let ρ_{AB} denote the joint initial state of Alice and Bob and σ_{AB} their joint state after the execution of the protocol, when Bob is allowed to do any deviation from the correct operation during the execution of P, averaged over all possible choices of random parameters by Alice. The protocol P is perfectly blind if*

$$\forall \rho_{AB} \in \mathcal{L}(\mathcal{H}_{AB}), \exists \mathcal{E} : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_B), \ s.t. \quad Tr_A(\sigma_{AB}) = \mathcal{E}(Tr_A(\rho_{AB})) \tag{1}$$

In the verification cryptographic setting Alice wants to delegate a quantum computation to Bob and accept or reject the result depending on whether the returned outcome is correct, or Bob has deviated [*]. This definition only concerns pure state inputs and unitary computations.

Definition 2 (Verifiability)**.** *A protocol for delegated computation is ϵ-verifiable ($0 \le \epsilon < 1$) if for any choice of Bob's strategy j, it holds that for any input of Alice:*

$$Tr(\sum_{\nu} p(\nu) P^{\nu}_{incorrect} B_j(\nu)) \le \epsilon \tag{2}$$

where $B_j(\nu)$ is the state of Alice's system A at the end of the run of the protocol, for choice of Alice's random parameters ν and Bob's strategy j. If Bob is honest we denote this state by $B_0(\nu)$. Let $P_{\perp}$ be the projection onto the orthogonal complement of the the correct quantum output. Then,

$$P^{\nu}_{incorrect} = P_{\perp} \otimes |ACC\rangle\langle ACC| \tag{3}$$

where $|ACC\rangle$ is the accept state for the indicator that Alice sets at the end of the protocol.

---

[*]In this work we will assume that the apparatuses of Alice and Bob are perfect. Without this assumption on Bob, the protocol will also detect any errors which may stem from Bob's faulty devices.

The main idea of the FK protocol is to test prover's honesty by hiding trap qubits among all qubits sent by verifier, in a way that they do not affect the result of the actual computation. Blindness means that prover cannot learn the position of the trap, nor its state. During the execution of the measurement based computation prover is asked to measure this trap qubit and report the result to verifier. If prover is honest this measurement gives a deterministic result, which can be verified by verifier and hence a dishonest sever will be detected with no-zero probability. Moreover the computation is encoded in a quantum error correcting code (QECC) correcting up to d errors, forcing malicious Bob to cause larger errors, if he is to interfere with the computation. These larger errors, in turn, are more easily detected.

Sketch of the FK protocol (Protocol 8 in [5])

1. Alice has a description of a computation in the measurement-based quantum computing (MBQC) model. She encodes the computation in a fault tolerant MBQC pattern, using a QECC that detects d errors.

2. Alice designs classically the embedding procedure of the encoded computation into a suitable MBQC pattern where the vertices can be divided into subsets S_γ where each subset contains a computational qubit and a trap qubit placed at a random position inside the subset. For the purpose of separating the computational and the trap qubits, special 'dummy' qubits prepared in the computational basis are injected.

3. Alice prepares all single qubits needed to construct the underlying entangled state for the pattern computation, pre-rotated by a random angle around Z axis in order to hide the measurement angle.

4. Bob receives the qubits one by one and entangles them to construct the underlying entangled state.

5. Alice sends to Bob at each step the measurement angles that implement the computation adapted based on the previous measurements results as well as cancelling the pre-rotation while adding a bit flip on the outcome to hide the measurement result.

6. Alice receives the measurement result and corrects it.

7. The isolated traps qubits are measured in the basis of their pre-rotated angles so the outcome is deterministic if Bob is honest.

8. At the end Alice accepts the outcome returned by Bob if all traps give the correct outcome.

In the following Lemma a distinction is made between the off-line phase of the protocol which Alice and Bob can execute before Alice receives the actual input, which is the description of the computation, and the on-line phase in which Alice and Bob repeatedly communicate to perform the measurements and corrections on the entangled state.

Lemma 1. *The FK protocol is perfectly blind (Theorem 12 in [5]) and ϵ-verifiable where $\epsilon = \frac{1}{c^{d_1}}$ (Theorem 13 in [5]) where d_1 is the number of errors detectable by the QECC used for amplification and some constant $c > 1$. The quantum requirement of Alice is to prepare single qubit states and the communication requirement is $\widetilde{O}(n^2) \times O(log(1/\epsilon))$ separable single qubit states sent from Alice to Bob off-line and $\widetilde{O}(n^2) \times O(log(1/\epsilon))$ bits of on-line classical communication between Alice to Bob, where n is the size of the computation.*

The number of of errors d_1 detectable by the QECC used for amplification will be referred to as the security parameter of the FK protocol in the rest of this paper.

In the ABE protocol the input is encoded by Alice using a secretly randomised QECC with specific properties that allow for the secret updating of the random key throughout the execution of the computation. It is then hard for Bob, without the knowledge of the key to deviate while keeping the state inside the legal subspace. The computation performed on the encoded input can be publicly announced without compromising the verifiability of the protocol.

Sketch of the ABE protocol (Protocol 4.2 in [6])

1. Alice has a description of a computation in the gate teleportation model where the non-Clifford operations are performed using non-Clifford magic states, Clifford gates and computational basis measurements.

2. She encodes the input (typically the blank state) to the computation in a qudit polynomial-QECC code and translates the computation to a logical one where a universal set of gates can be implemented transversally in this computation model. We refer to this public encoding of the computation as the public polynomial-QECC logical circuit.

3. She applies two layers of randomization on each logical input qudit: a random sign on each of the physical qudits, the same sign key is reused for all the different logical qudits, and a random Pauli rotation (different for each logical qudit).

4. Bob performs the computation while classically communicating with Alice to implement the corrections needed after each measurement step.

5. Alice receives the final output, undoes the quantum one time pad and the random sign key, using updated secret keys depending on the public polynomial-QECC logical circuit and the communication with Bob, and checks if it is inside the valid subspace of the code. If not, she rejects.

Lemma 2. *The ABE protocol is ϵ-verifiable where $\epsilon = \frac{1}{2^{d_2}}$ (based on Theorem 4.1 in [6] and ignoring the circuit error probability) where d_2 is the degree of polynomials in the polynomial-QECC. The quantum requirement of Alice is to prepare $O(n)$ states of $O(1/log(\epsilon))$ entangled qudits of $O(1/log(\epsilon))$-level and the communication requirement is $O(n)$ states of $O(log(1/\epsilon))$ entangled qudits sent from Alice to Bob off-line and $O(n) \times O(log(1/\epsilon))$ bits of on-line classical communication between Alice to Bob, where n is the size of the computation.*

The degree d_2 of polynomials used in the polynomial-QECC will be referred to as the security parameter of the ABE protocol in the rest of this paper.

2   Main results

We propose a new verification protocol that combines the techniques of the FK and ABE protocols. The main idea is to use the verifiable computation of the FK protocol to prepare on the prover's side the inputs encoded by the randomised polynomial QECC, that is, the states Alice would have to prepare and send in the first step of the original ABE protocol. On these states the public logical circuit of the ABE protocol is applied and the output is tested for being in the correct encoded subspace. If either of the trapification or decoding procedures fails, the verifier rejects.

The partitioning of the underlying resource state used in the FK protocol into smaller sub-states for each separable logical qudit leads to an improved communication complexity of the hybrid protocol compared to the original FK protocol.

In Section 2.1 we give an overview of how the FK protocol is modified for the needs of the preparation of the encoded state of the ABE protocol. Section 2.2 examines the problems of incorporating the computation and detection procedures of the ABE protocol into the hybrid protocol. In Section 2.3 we overview the hybrid protocol and how it achieves its improved complexity. The full description of the results is given in later sections and the detailed technical proofs are all in the Appendix.

2.1 Modifying the FK protocol for remote state preparation

We use the main detection and amplification technique of the FK protocol to remotely prepare the state needed for the ABE protocol on Bob's system. Due to blindness, Bob does not learn anything about this state and therefore any secret random parameters it contains, including a quantum one-time-pad with a key selected by Alice. The requirement for this state to be useful for the detection procedure of the ABE protocol is that it can be written in terms of the correct encoded state up to an arbitrary CPTP-map which does not depend on the secret parameters. We call such states verifiable states.

Two problems had to be tackled in modifying the FK protocol for this purpose. The first problem is that in the FK protocol, it is impossible to help the server distinguish the computational output systems from traps and dummies without jeopardizing the FK protocol's verifiability. We therefore construct a simple protocol to blindly transform the output of the FK protocol to the input that contains only the computational output system at a fixed position. Hence, Bob can apply the ABE protocol logical circuit on the output state while not learning anything about the trap qubits. Secondly, since the state at the end of the preparation phase does not contain any traps there is no possibility to test for the correctness of the output. However, since we only require a relaxed variant of verifiability (correctness up to a fixed CPTP map) this is proved not to be a problem by modifying the original proof of verification. The modified protocol with the localisation gadget we call the localising protocol.

Sketch of the localising protocol[†]

1. Alice and Bob follow the same steps as in the FK protocol, but an extra 'gadget' state (depicted in Figure 1) is attached on the output system qubits of the entangled state prepared by Bob for the original FK protocol. This gadget state does not contain any dummy or trap qubits on its final layer therefore effectively fixing the position of the output.

2. After all qubits of the normal entangled state are measured and the traps are tested Bob is asked to measure the remaining qubits in a way that only the output qubits are teleported to the last layer.

3. The state that Bob holds at the end is quantum one-time-padded with a key known only to Alice.

Theorem 1. *The output of the localising protocol after decoding of the QECC utilized in the FK protocol and decoding of the quantum one-time-pad, averaged over all random parameters of Alice, denoted as ν, is of the following form:*

[†]Full protocol is given in Section 4

$$\sum_\nu \rho_{out}^\nu \approx_\epsilon p_{acc}\mathcal{E}(|\psi_c\rangle\langle\psi_c|) \otimes |ACC\rangle\langle ACC| + (1 - p_{acc})\rho' \otimes |REJ\rangle\langle REJ|$$

where $\epsilon = \frac{1}{c^d}$ for some $c > 1$ and d the number of errors corrected by the FK protocol QECC, p_{acc} is a probability, $|\psi_c\rangle$ is the correct output of the computation, $\mathcal{E}$ is a CPTP-map where all Kraus operators are Pauli operators and is independent of $|\psi_c\rangle$ and ρ' is a normalized state.

It is important to note that using only a blind quantum computing protocol, without inserting any trap qubits for verification, one could not obtain the above required correct form for the final output system. In particular the possible cumulative perturbations that Bob may cause may be correlated to the state they act on, hence may not be expressible as a fixed CPTP map.

2.2 Incorporating the verification procedure of the ABE protocol

As mentioned before, in the hybrid protocol, Bob does not return the state to Alice after the localising protocol but he applies the polynomial-code logical circuit to implement the actual computation on the encoded state. In order to incorporate these extra steps we have to resolve a number of problems.

Firstly, the state that Bob holds is encoded by the QECC used for the amplification of the detection probability in the FK protocol. In order to apply the logical circuit of the ABE protocol on this state we need to ask Bob to decode the first QECC. Fortunately the QECC of the FK protocol is based on a stabiliser code with a Clifford decoding circuit [22]. The decoding circuit is publicly known and there is no need for any communication between Alice and Bob. An honest Bob performs the operators and Alice simply updates her quantum one-time-padding secret keys accordingly. Hence no information is leaked on the secret keys, also uniformity of the keys is preserved.

Secondly, the ABE protocol requires quantum states of prime dimension q where $q > 2$, whereas the original FK protocol uses qubits. To resolve this we present an analogue of the FK protocol which can use systems of any dimension while preserving all the security properties. The resources requirement for Alice is the same, the ability of preparing random single qudit states and the overall communication complexity remains the same as the original FK protocol.

Thirdly, since the computation we use from the ABE protocol is based on gate teleportation, there is a constant number of rounds of classical communication between Alice and Bob per non-Clifford gate teleportation. We prove, however, that this communication does not leak any of the secret parameters of the trapification phase, crucial for the security of the hybrid protocol.

Finally, we prove since the detection and decoding procedure that Alice applies to the returned state of the ABE protocol is a CPTP map, the resulting state of the overall protocol is ϵ-close to the final state of the ABE protocol, thus also verifiable.

Therefore we have the necessary tools to build a hybrid protocol by incorporating in the preparation stage (with the localising gadget) the application of the decoding part so that the assumptions of Theorem 2 can be modified to arrive to the desired verification property. However this protocol would not yet give any improvement in terms of complexity over the existing protocols and to achieve this an extra step has to be employed as we describe next.

2.3 Hybrid Protocol

We partition the underlying entangled state necessary for the FK protocol phase of the hybrid protocol into smaller separable sub-states preparing each a polynomial-QECC encoded input state

of the ABE protocol. Since the quadratic round complexity of the FK protocol comes from the complex structure of the overall required underlying resource state, simplifying the state for the purposes of this hybrid composition (observing that the polynomial-QECC encoded logical inputs are separable) succeeds in reducing the communication complexity. This modification does not violate the verification properties of the FK protocol since the fact that the states are separate is public knowledge and the detection and encoding procedures for each of the separate states can be done locally. The sketch of the hybrid protocol is given below:

Sketch of the FK-ABE hybrid protocol[‡]

1. Alice and Bob execute a specified number of instances of the qudit analogue of the FK protocol (that includes the localising gadget) to prepare in Bob's system each of the desired polynomial-QECC state of the ABE protocol.

2. Bob applies the publicly known Clifford decoding circuit for the QECC used for the amplification of the error detection probability of the FK protocol, and Alice updates her one-time-pad keys.

3. Alice and Bob apply the polynomial-QECC logical circuit on the encoded states following the steps of the ABE protocol. Alice updates her one-time-pad keys.

4. Bob sends the final measurement outcomes to Alice and Alice employs the detection and decoding procedure of the randomised polynomial-QECC (which is the final step of the ABE protocol as well).

Theorem 2. *Hybrid protocol is correct and ϵ-verifiable, with $\epsilon \leq \epsilon_1 + \epsilon_2$ where $\epsilon_1 = \frac{1}{c^{d_1}}$, $\epsilon_2 = \frac{1}{2^{d_2}}$ where d_1 and d_2 are the security parameters of the FK and ABE protocol phase of the hybrid protocol respectively and $c > 1$ is a parameter of the FK protocol phase. Alice needs only to prepare random single qudit states and the required classical and quantum communications is of order $O(nPolylog(\frac{1}{\epsilon}))$, where n is the size of the computation.*

The steps which are essential for the construction of this protocol can potentially be used for constructing different hybrid schemes.

3 Preliminaries

The FK protocol is defined in the measurement based quantum computing model (MBQC), basic elements of which are outlined in Section 3.1. The ABE protocol is a d-level quantum system protocol with $d > 2$ and is based on the Gate Teleportation Model outlined in Section 3.2. Finally the Quantum Error Correcting Code used in the ABE protocol is given in Section 3.3.

3.1 Measurement Based Quantum Computing

We introduce the notation necessary to describe a computation in MBQC [23, 24]. A generic computation consists of a sequence of commands acting on qubits:

- $N_i(|q\rangle)$: Prepare the single auxiliary qubit i in the state $|q\rangle$;

- $E_{i,j}$: Apply entangling operator cZ to qubits i and j;

[‡]Full protocol is given in Section 5

- M_i^α: Measure qubit i in the basis $\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - e^{i\alpha}|1\rangle)\}$ followed by trace out the measured qubit. The result of measurement of qubit i is called signal and is denoted by s_i;

- $X_i^{s_j}, Z_i^{s_j}$: Apply a Pauli X or Z correction on qubit i depending on the result s_j of the measurement on the j-th qubit.

The corrections could be combined with measurements to perform 'adaptive measurements' denoted as ${}^{s_z}[M_i^\alpha]^{s_x} = M_i^{(-1)^{s_x}\alpha + s_z\pi}$. A computation is formally defined by the choice of a finite set V of qubits, two not necessarily disjoint sets $I \subset V$ and $O \subset V$ determining the inputs and outputs, and a finite sequence of commands acting on V.

The entangling commands $E_{i,j}$ define an undirected graph over V referred to as (G, I, O). Along with the pattern we define a partial order of measurements and a dependency function D which is a partial function from O^C to $\mathcal{P}^{I^C}$, where $\mathcal{P}$ denotes the power set. Then, $j \in D_i^x$ if j gets a Pauli X correction depending on the measurement outcome of i and $j \in D_i^z$ if j gets a Pauli Z correction depending on the measurement outcome of i. A sufficient condition on the geometry of the graph state to allow unitary computation is the existence of flow ([25]). In what follows, $x \sim y$ denotes that x is adjacent to y in G.

Definition 3. *[25] A flow $(f, \preceq)$ for a geometry (G, I, O) consists of a map $f : O^c \mapsto I^c$ and a partial order $\preceq$ over V such that for all $x \in O^c$*

(F0) $x \sim f(x)$;

(F1) $x \preceq f(x)$;

(F2)   *for all $y \neq x, y \sim f(x)$: $x \preceq y$.*

3.2 d-level quantum operations and gate teleportation model

First we describe the d-level generalized gates that will be useful in the following constructions. All additions and multiplications in these definitions are performed modulo d, unless otherwise stated. The generalized Pauli operators over $\mathbf{F}_d$ are defined as: $X|a\rangle \equiv |a+1\rangle$, $Z|a\rangle \equiv \omega_d^a|a\rangle$, where $\omega_d = e^{2\pi i/d}$ is the primitive dth-root of unity. The generalized Hadamard (or Fourier) gate F is defined as:

$$|a\rangle \mapsto \frac{1}{\sqrt{d}} \sum_{b \in \mathbf{F}_d} \omega_d^{ab}|b\rangle.$$

The cX is defined as: $|a, b\rangle \mapsto |a, a+b\rangle$ and cZ as: $|a, b\rangle \mapsto \omega_d^{ab}|a, b\rangle$. The generalized phase gate S is defined as:

$$|a\rangle \mapsto \omega_d^{\frac{(a+1)a}{2}}|a\rangle$$

The generalized Toffoli gate which complements the set of Clifford gates to provide universality ([26], [27]) is defined as: $|a, b, c\rangle \mapsto |a, b, c + ab\rangle$. An alternative to the Toffoli gate to complement Clifford gates for universality is the family of 'so-called' generalized '$\pi/8$' gates [26] one of which, used in this paper, is defined as: $T|a\rangle \equiv \omega_d^{a^3}|a\rangle$ with the exception of qutrits where $T_3|a\rangle \equiv \omega_9^{(a^3 \bmod 9)}|a\rangle$.

In the gate teleportation model the ABE protocol is defined in, all Clifford gates are performed by applying unitary operators, while the non-Clifford gates are performed by entangling with magic

non-Clifford states (Toffoli states in the case of the ABE protocol), measuring in the computational basis and performing Clifford correction operators on the remaining states [28].

3.3 Polynomial Quantum Error Correcting Code

The class of quantum error correcting codes used in the ABE protocol, is based on polynomial error-correcting codes [29]. By randomizing these codes using a secret sign key one can acquire a Quantum Authentication Scheme (QAS) [30], usable by two parties who want to authenticate a quantum state exchanged through a malicious quantum channel. Due to specific properties of the *signed* polynomial error-correcting codes, they can also be used in the context of secure quantum multiparty computation [31] and in the context verification of a single quantum prover as demonstrated in the ABE protocol.

Specifically, the code operates over the field $\mathbf{F}_d$, where d is prime and represents the dimension of the quantum system. The code uses polynomials $f(\cdot)$ with coefficients from $\mathbf{F}_d$ and with a maximum degree of p, where p is a parameter of the code. These polynomials are evaluated at m *distinct non-zero points* from $\mathbf{F}_d$: $\{a_1 \ldots a_m\}$. To be able to choose m distinct non-zero points from $\mathbf{F}_d$ we impose the restriction: $m < d$. Moreover, we set $m = 2p + 1$. Finally, the code uses a secret sign key that is a uniformly randomly chosen string $\mathbf{k} \leftarrow \{\pm 1\}^m$.

Given a quantum state $|a\rangle$, where $a \in \mathbf{F}_d$, we can encode it using the signed polynomial error-correcting code:

$$|a\rangle \rightarrow \frac{1}{\sqrt{q^p}} \sum_{\{f | deg(f) \leq p, f(0)=a\}} |(k_1 f(a_1), \ldots, k_m f(a_m)) \mod d\rangle$$

where the mod d is taken element-wise in the label of the right-hand side ket.

To detect if there was any Pauli error in the transmitted codeword, the receiver undoes the sign key and checks if the resulting string is the representation, at m distinct points, of a polynomial of maximum degree p. If not it aborts and declares the state invalid. The probability of accepting an incorrect state (when the channel applies an arbitrary Pauli attack) is exponentially small on p. In order to acquire the same property for any type of malicious attack, an extra quantum one-time-pad is added on top of the existing randomization, as it is the case in the ABE protocol.

4 Localising Protocol

In this section we give an explicit description of the localising protocol. The core methodology is the same as in the FK protocol. Each trap is prepared in state $|+_{\theta_t}\rangle$, where θ is chosen at random from angle set $A = \{0, \pi/4, 2\pi/4, \ldots, 7\pi/4\}$, and placed at position t in the graph. Positions t are such that for the graph used in the FK protocol there exists a partitioning into sub-graphs S_γ that the each trap is placed at a uniform random position inside each S_γ. In the FK protocol the graph that is used to achieve this property is the dotted-complete graph [5], while other graphs can possibly satisfy the same property. In order to separate the qubits participating in the computation and the trap qubits, dummy qubits prepared in the computational basis are placed between them so that the corresponding entangling operators have no effect. The choice of the basis for each dummy state is uniformly random to satisfy the blindness property. In particular, if a dummy qubit is in state $|0\rangle$, applying the entangling operator cZ between this qubit and a qubit prepared on the (X, Y) plane has no effect. If a dummy qubit is in state $|1\rangle$ then applying cZ will introduce a Pauli Z rotation on the qubit prepared on the (X, Y) plane. This effect can be cancelled by Alice in advance, by introducing a Pauli Z rotation on all the neighbours of $|1\rangle$'s when preparing the initial state.

Protocol 1 Localising Protocol (based on the FK protocol)

Alice's input. Description of a computation in the MBQC model (or equivalent) using a convenient underlying open graph state (G, I, O). The computation is represented, for any qubit $i \in G \setminus O$, as a measurement angle φ_i (together with the set of X-dependences D_i^X and Z-dependences D_i^Z and a fixed partial order of measuring depending on the graph structure). The input is set to be the Hadamard basis state of n qubits: $|+\rangle^{\otimes n}$. Protocol can be extended to admit external quantum input by applying the techniques described in the FK protocol.

Bob's output. A quantum state that contains the encoded and one time padded quantum output of the computation.

The protocol

1. Preprocessing 1. Alice translates the computation to a Fault Tolerant (FT) MBQC pattern that can detect d errors. Let the updated open graph be (G', I', O'), where $|G| = m'$ and $|I'| = |O'| = n'$.

2. Preprocessing 2. Alice embeds the encoded computation pattern into a suitable graph which has the following property: There exists a fixed order of measurement which respects the computational flow and each computational qubit belongs to a constant size subset of qubits S_γ in which a trap can be at any position with uniformly random probability. An example is the dotted complete graph of size $O(m'^2)$.

3. Preprocessing 3. Alice attaches a gadget graph (Figure 1) on each subset S_γ of qubits of the output system of the previous step's graph. The effect of these extra graphs is that they fix the position of system O'. The total number of qubits of the final graph is N.

4. Alice prepares the rotated qubits. For $i = 1$ to N:

   (a) If qubit is a dummy: prepares $|d_i\rangle$, $d_i \leftarrow_R \{0, 1\}$ (where $\leftarrow_R$ means *chosen uniformly at random from*).

   (b) If qubit is not dummy and not in O': prepares $\prod_{j \in N_G(i) \cap D} Z^{d_j} |+_{\theta_i}\rangle$, where $|+_{\theta_i}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_i}|1\rangle)$, $\theta_i \leftarrow_R \{0, \pi/4, 2\pi/4, \dots, 7\pi/4\}$.

   (c) If qubit is in O': Same as previous step but θ is fixed to 0 and an extra Z^{r_i} rotation is applied where r_i is a random bit.

   (d) She sends the qubit to Bob.

5. Bob entangles the states according to the graph state by applying cZ gates.

6. Bob performs the rest of the computation using classical help from Alice. For i which ranges over all qubits (respecting the flow) except system O':

   (a) Alice computes the actual measurement angle ϕ_i' using the dependences and the previous measurement results ($\phi_i = 0$ for dummies and traps).

   (b) Alice chooses a random bit r_i and computes $\delta_i = \phi_i' + \theta_i + \pi r_i$.

   (c) Alice transmits δ_i to Bob.

   (d) Bob performs measurement $M_i^{\delta_i}$ on qubit i.

   (e) Bob transmits the result to Alice.

   (f) Alice flips the result if $r_i = 1$, otherwise does nothing.

7. Alice sets her indicator bit to accept if all trap tests where successful.

During the execution of measurement based computation Bob is asked to measure the trap qubits, at positions $t \in T$, each with angle $\theta_t + r\pi$ and return each classical result b_t to Alice. If for all trap qubits $t \in T$ we have $b_t = r_t$ Alice sets an indicator bit to state acc (which means that this computation is accepted), otherwise she sets it to rej (computation is rejected). Due to blindness (achieved by the random rotations) the prover cannot learn the position of traps so he is not able to return with probability one the correct results of the trap measurements while deviating from the steps of the protocol. The computation is encoded in a fault tolerant procedure using a QECC that can perfectly correct d errors, so dishonest prover has to attack at more than d positions, thus having exponentially small in d probability of succeeding in predicting the correct results of the corresponding traps.
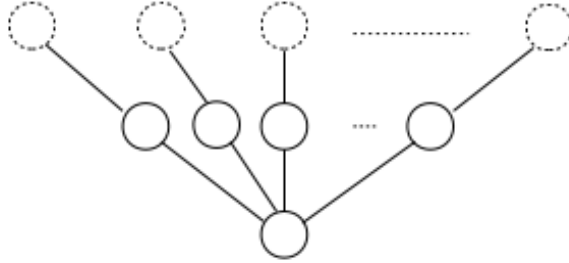

Figure 1: Single gadget state attached to a subset S_γ (represented by dashed circles) of the output of the normal graph used in the FK protocol. The number of branches depends on $|S_\gamma|$. Only one of the qubits of the first row of the gadget is a non-dummy state allowing to teleport blindly the actual output to the bottom qubit.

The main difference from the original FK protocol is the modification of the graph state by appending on the output a specific number of gadget states, one of which is depicted in Figure 1. Specifically one gadget is attached on each subset S_γ of the output of the FK protocol graph (system to be normally returned to Alice). Following the construction in the FK protocol, we assume that each S_γ contains one trap qubit, a number of dummy qubits and one qubit participating in the actual computation (in the dotted-complete graph based version of the FK protocol $\forall \gamma, |S_\gamma| = 3$). The goal of the gadget system is to teleport only the computational qubit to the fixed vertex at the bottom of each gadget. Therefore the first layer of the gadget qubits (in Figure 1 the first row of solid circles, that are connected directly to the existing graph of the FK protocol) contains $|S_\gamma| - 1$ dummy qubits which isolate the trap and the dummies of the output S_γ from the bottom qubit. The computational qubit and the gadget qubit that is connected to it are both measured with $\phi = 0$ so that the effective computation is identity and the qubit is teleported to the bottom of the gadget. The gadget structure is such (one gadget per S_γ and symmetric) that they can be added without breaking the uniformity of the positioning of the traps in the FK protocol graph. The steps of the localising protocol are given in Protocol 1.

A sketch of the proof of verifiable state preparation, formally described in 1, is given here, while a detailed proof is presented in Appendix A.

The following lemma will be used in the proof:

Lemma 3. *(Channel twirling [32])*

12

$$\sum_i P_i Q P_i \rho P_i Q' P_i = 0, \ \ if \ Q \neq Q' \tag{4}$$

where ρ is a matrix, Q, Q' are two arbitrary general Pauli operators of the same dimension, and $\{P_i\}$ is the set of all general Pauli operators of dimension same as Q and Q'.

Extra notation has to be introduced first. Vector ν is used to represent all random secret parameters chosen by Alice throughout the execution of protocol, including $\boldsymbol{r} = \{r_i\}$, $\boldsymbol{\theta} = \{\theta_i\}$, $\boldsymbol{d} = \{d_i\}$ and positions of traps $\boldsymbol{t} = \{t_i\}$. Parameter $p(\nu)$ gives the probability of a particular choice of random secret parameters. Summing over a vector (e.g. $\sum_{\boldsymbol{r}}$) means that we sum over all possible choices for the elements of that vector (e.g. all possible bit-strings of size N for $\boldsymbol{r}$).

For convenience we denote some of the subsystems of the joint Alice-Bob state:

- System $\mathcal{M}$ contains the qubits of the graph state that participate in the computation and are measured.

- System D contains all dummy qubits.

- System T contains all trap qubits.

- System O' is the fixed output system (therefore all the bottom qubits of the gadget states - which are the only that are not measured).

- System Δ is the system of the measurement angles send by Alice to Bob, where each angle is represented by three qubits in the computational basis.

- System B is Bob's private system, assumed to be initially in the blank state.

Proof Sketch of Theorem 1 *(Preparation of verifiable states by the localising protocol.)* We follow a single index convention to enumerate the qubits participating in the graph where N is the total number of qubits and the last n' qubits are the qubits which are not measured (system O'). While in Protocol 1 system O' remains to the hands of Bob, to be used for the next phase of the hybrid protocol, to prove the property of Theorem 1 we have to assume extra steps of Alice receiving and decoding the output state. As it will be made clear in the next section, the same property is true in the case Bob applies an extra Clifford circuit, which is needed in FK-ABE hybrid protocol, before returning the state to Alice.

Honest computation includes global entangling operator E_G (Step 5) on the received state $|M(\boldsymbol{\theta}, \boldsymbol{d}, \boldsymbol{t})\rangle$ (all qubits sent at Step 4) and for each $1 \leq i \leq N - n'$ a measurement, described in Step 6d, with outcome $b_i \in \{0, 1\}$. This measurement can be analysed into unitary part $H_i R_i(\delta_i)$, where H_i is the Hadamard gate and $R_i(.)$ is rotation around z-axis on qubit i which depends on measurement angles $\boldsymbol{\delta}(\boldsymbol{\theta}, \boldsymbol{r}, \boldsymbol{b})$ (where $\boldsymbol{b} = (b_i)_i$), and a Pauli Z measurement on qubit i (projectors $|b_i\rangle\langle b_i|$). Without loss of generality we can represent any dishonest behaviour of Bob at any step as applying the correct unitary operators and then an arbitrary unitary attack operator which applies also on his private system assumed to be in state $|0\rangle^{\otimes B}$.

After trivial commutations, the output of Protocol 1, with extra steps of Alice receiving system O' and applying decoding map $\mathcal{D}$ for the FK protocol QECC and final Pauli corrections $C(\boldsymbol{r}, \boldsymbol{b})$, which include output system corrections $C_{O'}$ and trap results corrections by r_t, can be written as (note that we omit the dependences of each operator in the formula for the sake of brevity):

$$\rho_{out} = Tr_{B,\mathcal{M},\Delta,D}(\sum_{\boldsymbol{b}}\sum_{\nu} p(\nu)C\mathcal{D}(|\boldsymbol{b}\rangle\langle\boldsymbol{b}|U(H_{N-n'}R_{N-n'}(.)\ldots H_1 R_1(.)E_G($$

$$|M\rangle\langle M| \otimes |\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|)E_G R_1(.)^\dagger H_1 \ldots R_{N-n'}(.)^\dagger H_{N-n'} \otimes |0\rangle\langle 0|^{\otimes B})U^\dagger|\boldsymbol{b}\rangle\langle\boldsymbol{b}|)C^\dagger) \tag{5}$$

where U is the global (commuted) unitary attack operator that is chosen by Bob and applies on system $\mathcal{M} \times O' \times D \times \Delta \times B$.

Tracing out system B, attack U ($U^\dagger$) is transformed to a Completely Positive Trace Preserving (CPTP) map acting on the remaining system. We can write the CPTP map in the Kraus decomposition and express the Kraus operators in the Pauli basis (all possible tensor products of single qubit Pauli operators). Moreover, applying the part of the honest unitary operation for each trap (entangling with its neighbour dummy qubits and $H_t R_t(\delta_t)$) results in the system of traps T being disentangled from the rest. The remaining unitary operators are denoted by $\mathcal{P}' \equiv H_{N-n'}R_{N-n'}(.)\ldots H_1 R_1(.)E'_G$ and the remaining system that they apply to is denoted by $|M'\rangle$.

$$\rho_{out} = Tr_{\mathcal{M},\Delta,D}(\sum_{\boldsymbol{b}}\sum_{\nu} p(\nu) \sum_{k,u,v,u',v'} a_{k,u,v}a^*_{k,u',v'}C_{O'}\mathcal{D}(|\boldsymbol{b}'\rangle\langle\boldsymbol{b}'|P_{u|i:\forall j,i\neq t_j} \otimes P_v$$

$$(\mathcal{P}'(|M'\rangle\langle M'| \otimes |\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|)\mathcal{P}'^\dagger)P_{u'|i:\forall j,i\neq t_j} \otimes P_{v'}|\boldsymbol{b}'\rangle\langle\boldsymbol{b}'|)C^\dagger_{O'}$$

$$\bigotimes_i |b_{t_i} + r_{t_i}\rangle\langle b_{t_i}|P_{u|t_i}|r_{t_i}\rangle\langle r_{t_i}|P_{u'|t_i}|b_{t_i}\rangle\langle b_{t_i} + r_{t_i}|)) \tag{6}$$

where

- $a_{k,u,v}$ are complex numbers, with $\sum_{k,u,v} |a_{k,u,v}|^2 = 1$.

- P_u (and $P_{u'}$) ranges over all tensor products of Pauli operators on the system that is trapified: all qubits of system $\mathcal{M} \times D \times T$ except the qubits that belong to the gadget and are measured (first row of each gadget).

- P_v (and $P_{v'}$) ranges over all tensor products of Pauli operators on the system that is not trapified: all qubits that belong to gadget systems and the measurement angle system Δ.

- $P_{u|i}$ is the i-th Pauli element of P_u.

- $\boldsymbol{b}'$ is the vector that is generated from $\boldsymbol{b}$ by removing elements $\{b_{t_i}\}$.

So far, the analysis followed similar techniques to verifiability proof of the original FK protocol. However the following steps have to be introduced to take care of the issues of using the extra gadget state and not having traps on the final output state (therefore proving the relaxed verification requirement).

Summing over random parameters $\boldsymbol{\theta}$, $\boldsymbol{d}$ and $\boldsymbol{r}$ and tracing over systems Δ, D and $\mathcal{M}$ respectively enables us, with the aid of Lemma 3, to eliminate all terms where $P_{u|i} \neq P_{u'|i}$ and $P_{v|i} \neq P_{v'|i}$ which reduces the attack of Bob on the remaining state $\mathcal{P}^{(3)}|M^{(3)}\rangle$ (where all dependences on these random parameters is eliminated - corrections on the output are also updated accordingly to $C'_{O'}$) to a convex combination of Pauli operations.

$$\rho_{out} = \sum_{\boldsymbol{b}} \sum_{\boldsymbol{t}} p(\boldsymbol{t}) \sum_{k,u,v} |a_{k,u,v}|^2 C'_{O'} \mathcal{D}(\langle \boldsymbol{b}'|P_{u|i:\forall j,i\neq t_j} \otimes P_{v|O''}$$

$$(\mathcal{P}^{(3)}(|M^{(3)}\rangle\langle M^{(3)}|)\mathcal{P}^{(3)\dagger})P_{u|i:\forall j,i\neq t_j} \otimes P_{v|O''}|\boldsymbol{b}'\rangle)C'_{O'} \bigotimes_i P_{u|t_i}|0\rangle\langle 0|P_{u|t_i} \tag{7}$$

where O'' is the system that contains the qubits of all gadgets.

We split the terms of the sum over the attack operators P_u into the terms which are deterministically corrected by $\mathcal{D}$ and the terms that are not corrected by $\mathcal{D}$ but with high probability will have an effect on the trap measurement outcomes signifying that an attack has happened.

Specifically, we first examine state σ_1 which comes from ρ_{out} by restricting summation to $u \in \mathcal{S}_1$, where $\mathcal{S}_1$ is the set of tensor products of Pauli operators that contain $\leq d$ elements with Pauli X component (d is the number of correctable errors of the code). Attacks $P_{v|O''}$ on the output gadget can be rewritten as Pauli attacks on the output state O' that are not correlated on the state itself. This is possible only because Pauli attacks on the last measurement layer of MBQC can be translated to corrections on the output, which is not the case for attacks on any layer. Moreover, attacks $P_{u|i:\forall j,i\neq t_j}$ will be perfectly corrected when applying $\mathcal{D}$, since their footprint is $\leq d$, giving correct output state $|\psi_c\rangle$. Separating the attacks to those who have an effect on the trap system, causing Alice to set her indicator bit to $|REJ\rangle$, and those who do not touch any trap (and therefore Alice accepts) we get:

$$\sigma_1 = \sum_i p'_i P_i |\psi_c\rangle\langle\psi_c|)P_i \otimes |ACC\rangle\langle ACC| + \sum_j p''_j P_j |\psi_c\rangle\langle\psi_c|P_j \otimes |REJ\rangle\langle REJ| \tag{8}$$

where P_i (P_j) range over all tensor products of Pauli operators on the output system O and p'_i, p''_i are probabilities, with $\sum_i (p'_i + p''_i) = \sum_{k,u\in\mathcal{S}_1,v} |a_{k,u,v}|^2$.

Let state σ_2 include remaining terms of the summation over u in Equation 7, where $u \in \mathcal{S}_2$ corresponds to P_u where $> d$ Pauli elements have Pauli X component.

We calculate the probability the state collapses to the 'incorrect' subspace $P_\perp = I - |\psi_c\rangle\langle\psi_c|$ and all the trap measurement outcomes returned are correct. Since Bob has to guess the output of the trap measurement at, at least, d positions, where the traps can be placed with probability that depends on the amount of traps in the graph, the probability of cheating successfully is exponentially decaying in d.

$$Tr(P_\perp \bigotimes_i |0\rangle_i\langle 0|_i \sigma_2) \leq \sqrt{(1/c)^d} \tag{9}$$

where $c > 1$ is a constant that depends on the ratio of total qubits and traps in the graph. Therefore state σ_2 can be written as:

$$\sigma_2 \approx_\epsilon p_1 |\psi_c\rangle\langle\psi_c| \otimes |ACC\rangle\langle ACC| + p_2\rho \otimes |REJ\rangle\langle REJ| \tag{10}$$

where $\epsilon = \sqrt{(1/c)^d}$, p_1 and p_2 are probabilities with $p_1 + p_2 = \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2$ and ρ is a density matrix.

Summing again the terms σ_1 and σ_2, theorem is satisfied for $\epsilon = \sqrt{(1/c)^d}$.

$\square$

5 Hybrid Protocol

The proposed FK-ABE hybrid protocol combines all the techniques discussed so far, including the partitioning of the high complexity resource state of the FK protocol to sub-graphs, each used for the preparation of a separate encoded state for the ABE protocol, thus reducing the quantum and classical communication complexity.

The protocol, described here as Protocol 2, is based on a d-level version of Protocol 1, for d odd prime, which corresponds to the following changes:

- The state is entangled by applying generalized cZ gates.

- Alice's states $|+_{\theta_i}\rangle$ are replaced by states $T^{c_i} S^{b_i} Z^{a_i} \frac{1}{\sqrt{d}}(|0\rangle + \ldots + |d-1\rangle)$, where T are generalized '$\pi/8$' gates, S generalized phase gates, Z generalized Pauli Z gates and $a_i, b_i, c_i \leftarrow_R \mathbf{F}_d$ (except qutrits, where T gate is replaced by T_3 gate and $c_i \leftarrow_R \mathbf{F}_9$).

- Dummy states are generalized computational basis states $|d_i\rangle$, $d_i \leftarrow_R \mathbf{F}_d$

- Measurements on vector $(a_i', b_i', c_i') \in \mathbf{F}_d^3$ correspond to generalized measurements on basis $\{Z^j T^{c_i'} S^{b_i'} Z^{a_i'} \frac{1}{\sqrt{d}}(|0\rangle + \ldots + |d-1\rangle)\}_{j=0}^{d-1}$. Measurements vectors are corrected to incorporate generalized Pauli X and Z corrections [33],[34] according to flow dependencies.

- Alice cancels the pre-rotation by adding (a_i, b_i, c_i) on her (corrected) measurement vector. In the measurement vector she sends to Bob, extra term $(r_i, 0, 0)^T$, $r_i \leftarrow_R \mathbf{F}_d$ is added to randomize the output of Bob's measurement. She corrects the measurement result she receives from Bob by adding r_i.

Correctness of the d-level version of the FK protocol follows the same argument of the correctness of qubit case, applying d-level MBQC [33],[34] and noticing that the d-level dummy qudits have the same effect as in the qubit case. Universality comes from the fact that we are able to perform a universal set of gates for d-level computation: $\{cX, F, S, T, Z\}$ [26], with the special case of qutrits where T becomes T_3.

A sketch of the proof of verifiability of Protocol 2 is given here, while a detailed proof is presented in Appendix B.

We use the same notation as in the proof of Theorem 1 to denote the different subsystems, however there is a new subsystem denoted by $\mathcal{L}$ that contains the corrections sent from Alice to Bob for the Toffoli gate implementation at the ABE protocol phase. System $\mathcal{M}$ still contains the qudits of the graph state that participate in the computation and are measured during the application of the FK protocol stage but not the qudits that are measured during the ABE protocol phase.

Proof Sketch of Theorem 2 *(Verifiability of FK-ABE hybrid protocol)*. We employ similar techniques to those in Theorem 1 to write the state of Alice, before applying the detection mechanism of the ABE protocol, as a verifiable state, for any choice of the random sign key and without leaking information about it.

The extra elements that FK-ABE hybrid protocol introduces, compared to the localising protocol, include the measurements needed for the implementation of the Toffoli gates, with outcomes $\widetilde{b}_i \in \mathbf{F}_d$ sent from Bob to Alice and corrections $\widetilde{r}_i \in \mathbf{F}_d$ sent from Alice to Bob. The Clifford circuit that implements the logical public circuit of the ABE protocol is denoted by $\mathcal{C}$ and applies on the decoded for the FK protocol QECC output system O and on the corrections system $\mathcal{L}$. Final Pauli corrections $C''(\boldsymbol{r}, \boldsymbol{b}, \widetilde{\boldsymbol{b}})$ for Alice, here, take also into account the update due to the application of $\mathcal{C}$ and include output system corrections $C''_{O'}$ and trap results corrections by r_t. Note that the qubit

---
Protocol 2 FK-ABE Hybrid Protocol

Alice's input. Description of a computation in the Gate Teleportation model based on generalized Toffoli states. The input is set to be the Fourier basis state of n qudits: $|+_0\rangle^{\otimes n}$, where $|+_0\rangle = \frac{1}{\sqrt{d}} \sum_a |a\rangle$. The total number of gates is denoted by t. Protocol can be extended to admit arbitrary quantum input using the same methods as in the FK protocol.

Alice's output. The result of measurement of the quantum output of the circuit and a bit indicating if the result is accepted or not.

The protocol

1. Alice chooses a single random sign key (of size equal to the size of a codeword) that will be used to encode all inputs (including Toffoli states) according to the signed-polynomial QECC.

2. A d-level Fault Tolerant QECC is selected for amplification of the detection probability of the FK protocol.

3. Alice has to remotely prepare the Toffoli states and to encode both the inputs and the Toffoli states according to the ABE protocol QECC randomized by the selected sign key. For each encoded state she selects a separate graph state that has the properties described in Protocol 1. Therefore, the size of each sub-graph depends only on the security parameters of the protocol and not on the size of the computation t.

4. Alice and Bob encode all inputs (including Toffoli states) by executing Protocol 1 adapted for d level systems. The output of Bob is encoded by the QECC used for amplification of the FK protocol and the final quantum one time pad, which depends on the secret parameters of the FK protocol and will referred to as the Pauli key. Alice holds an indicator bit set on accept or reject depending on the outcome of the traps.

5. Bob applies the Clifford circuit for decoding the QECC used for amplification of the FK protocol and Alice updates her Pauli keys accordingly.

6. Alice and Bob perform the logical operators that correspond to the desired computation on the encoded by polynomial QECC state as described in the ABE protocol. For each application of logical Toffoli gate, Bob sends measurement results to Alice and Alice calculates the actual correction to be performed on the state and sends it to Bob who performs it.

7. Bob measures the output qudits in the computational basis and returns the measurement results to Alice.

8. Alice applies the detection and decoding procedure of the signed polynomial QECC and sets a second indicator bit accordingly.

9. Alice accepts if both indicator bits of the FK and ABE protocol phase of the protocol are set to accept, otherwise she rejects.

---

gates have been replaced by their d-level analogues. To highlight the analogy with the qubit case we keep the same notation of the measurement vectors: $\boldsymbol{\theta}, \boldsymbol{\phi}$ and $\boldsymbol{\delta}$, noting that they are dit instead of bit triples. We can, therefore, write Alice's final output before the detection mechanism of the ABE protocol phase as:

$$\rho_{out} = Tr_{B,\mathcal{M},\Delta,D,\mathcal{L}}(\sum_{\boldsymbol{b},\widetilde{\boldsymbol{b}}}\sum_{\nu} p(\nu) C''(|\boldsymbol{b}\rangle\langle\boldsymbol{b}| \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|UC\mathcal{D}(F_{N-n'}R_{N-n'}(.)\ldots F_1R_1(.)E_G($$

$$|M\rangle\langle M| \otimes |\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|)E_G R_1(.)^\dagger F_1^\dagger \ldots R_{N-n'}(.)^\dagger F_{N-n'}^\dagger \otimes |0\rangle\langle 0|^{\otimes B} \otimes |\widetilde{\boldsymbol{r}}\rangle\langle\widetilde{\boldsymbol{r}}|)\mathcal{D}^\dagger\mathcal{C}^\dagger U^\dagger |\boldsymbol{b}\rangle\langle\boldsymbol{b}| \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|)C'')\quad(11)$$

where U represents global (commuted) Bob's attack that in this case applies also on system $\mathcal{L}$. Similarly to proof of Theorem 1 Alice's output can be rewritten as:

$$\rho_{out} = Tr_{\mathcal{M},\Delta,D,\mathcal{L}}(\sum_{\boldsymbol{b},\widetilde{\boldsymbol{b}}}\sum_{\nu} p(\nu) \sum_{k,u,v,u',v'} a_{k,u,v}a^*_{k,u',v'}C''_{O'}(|\boldsymbol{b}'\rangle\langle\boldsymbol{b}'| \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|P_{u|i:\forall j,i\neq t_j} \otimes P_v$$

$$\mathcal{C}\mathcal{D}(\mathcal{P}'(|M'\rangle\langle M'| \otimes |\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|)\mathcal{P}'^\dagger)\mathcal{D}^\dagger\mathcal{C}^\dagger P_{u'|i:\forall j,i\neq t_j} \otimes P_{v'}|\boldsymbol{b}'\rangle\langle\boldsymbol{b}'| \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|)C''^\dagger_{O'}$$

$$\bigotimes_i |b_{t_i}+r_{t_i}\rangle\langle b_{t_i}|P_{u|t_i}|r_{t_i}\rangle\langle r_{t_i}|P_{u'|t_i}|b_{t_i}\rangle\langle b_{t_i}+r_{t_i}|))\quad(12)$$

where the only difference from the proof of Theorem 1 is that the attacks P_u (and $P_{u'}$), P_v (and $P_{v'}$) are tensor products of d-level Pauli operators and that P_v (and $P_{v'}$) applies also on system $\mathcal{L}$.

Again, summing over random parameters $\boldsymbol{\theta}$, $\boldsymbol{d}$ and $\boldsymbol{r}$ and tracing over systems Δ, D and $\mathcal{M}$ respectively enables us to reduce the attack on these systems to a mixture of Pauli operations. Special care has to be taken for the attack on system $\mathcal{L}$ which can be reduced to Pauli operators by exploiting the structure of the Toffoli implementation circuit, where all logical measurements have uniformly random results, and, therefore, an extra logical Pauli X randomization can be extracted. Tracing out the system $\mathcal{L}$ as well results to:

$$\rho_{out} = \sum_{\boldsymbol{b},\widetilde{\boldsymbol{b}}}\sum_{\boldsymbol{t}} p(\boldsymbol{t}) \sum_{k,u,v} |a_{k,u,v}|^2 C^{(3)}_{O'}(\langle\boldsymbol{b}'| \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|P_{u|i:\forall j,i\neq t_j} \otimes P_{v|O''}$$

$$(\mathcal{C}\mathcal{D}(\mathcal{P}^{(3)}(|M^{(3)}\rangle\langle M^{(3)}|)\mathcal{P}^{(3)\dagger})\mathcal{D}^\dagger\mathcal{C}^\dagger)P_{u|i:\forall j,i\neq t_j} \otimes P_{v|O''}|\boldsymbol{b}'\rangle \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|)C^{(3)\dagger}_{O'} \bigotimes_i P_{u|t_i}|0\rangle\langle 0|P_{u|t_i}\quad(13)$$

The next step is the splitting of the internal sum (over u) into two parts, yielding two sub-normalized states σ_1 and σ_2. In σ_1 we restrict the index u to the set S_1, which contains all attacks which are corrected by the FK protocol QECC, with parameter d_1, and in σ_2 to $u \in \mathcal{S}_2$ which contains attacks with Pauli X footprint $> d_1$ and therefore will activate at least d_1 traps when averaging over all positions for the traps. The only difference here from the proof of Theorem 1 is the existence of the public circuit $\mathcal{C}$, but since it applies only on system O it does not affect the probabilities of detecting the traps and since it is Clifford the Pauli corrections commute with it and get updated secretly by Alice. Again:

$$\sigma_1 = \sum_i p'_i P_i|\psi'_c\rangle\langle\psi'_c|P_i \otimes |ACC_1\rangle\langle ACC_1| + \sum_j p''_j P_j|\psi'_c\rangle\langle\psi'_c|P_j \otimes |REJ_1\rangle\langle REJ_1|\quad(14)$$

where $|\psi_c'\rangle\langle\psi_c'|$ is the correct state after the ABE protocol phase is performed and the quantum one time pad with the Pauli key is undone. Also P_i (P_j) range over all tensor products of d-level Pauli operators on the output system O and p_i', p_i'' are probabilities, with $\sum_i(p_i'+p_i'') = \sum_{k,u\in\mathcal{S}_1,v}|a_{k,u,v}|^2$.

Also, since the same counting arguments hold for the d-level traps on the measured system:

$$\sigma_2 \approx_{\epsilon_1} p_1|\psi_c'\rangle\langle\psi_c'|\otimes|ACC_1\rangle\langle ACC_1| + p_2\rho\otimes|REJ_1\rangle\langle REJ_1| \tag{15}$$

where $\epsilon_1 = \sqrt{(1/c)^{d_1}}$, $p_1 + p_2 = \sum_{k,u\in\mathcal{S}_2,v}|a_{k,u,v}|^2$ and ρ is a density matrix.

By adding the states described in Equations 14 and 15 and by contractiveness of the ABE protocol detection procedure that Alice applies to check if the state is in the valid space of the signed polynomial QECC, theorem is satisfied for $\epsilon_1 = \sqrt{(1/c)^{d_1}}$ and $\epsilon_2 = (1/2)^{d_2}$, where d_2 is the degree of the polynomials in the QECC used in the ABE protocol.

$\square$

In the FK-ABE hybrid protocol the quantum requirement for Alice is to prepare single qudit states of the form $T^{c_i}S^{b_i}Z^{a_i}|+_0\rangle$, for $a_i, b_i, c_i \leftarrow_R \mathbf{F}_d$, where d is an odd prime. The dimension d of each system is $O(1/log(\epsilon))$. Alice has to send to Bob, at the beginning of the protocol before getting the computation description, $O(n\mathrm{Polylog}(\frac{1}{\epsilon}))$ separable single qudit states, where n is the size of the computation. After, Alice and Bob have to exchange only classical information in $O(n\mathrm{Polylog}(\frac{1}{\epsilon}))$ rounds, where each round includes a constant size message sent from Bob to Alice and a constant size message from Alice to Bob.

Acknowledgements

References

[1] Dorit Aharonov and Umesh Vazirani. *Is Quantum Mechanics Falsifiable? A computational perspective on the foundations of Quantum Mechanics.* 2012.

[2] A.Childs. Secure assisted quantum computation. *Quant. Inf. Compt.*, 5(6):456, 2005.

[3] Pablo Arrighi and Louis Salvail. Blind quantum computation. *International Journal of Quantum Information*, 4(05):883–898, 2006.

[4] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

[5] Joseph F Fitzsimons and Elham Kashefi. Unconditionally verifiable blind computation. *arXiv preprint arXiv:1203.5217*, 2012.

[6] Dorit Aharonov, Michael Ben-Or, and Elad Eban. Interactive proofs for quantum computations. In *Proceedings of Innovations in Computer Science 2010*, ICS2010, pages 453–, 2010.

[7] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.

[8] Anne Broadbent, Gus Gutoski, and Douglas Stebila. Quantum one-time programs. In *Advances in Cryptology–CRYPTO 2013*, pages 344–360. Springer, 2013.

[9] Tomoyuki Morimae and Keisuke Fujii. Blind quantum computation protocol in which alice only makes measurements. *Physical Review A*, 87(5):050301, 2013.

[10] Scott Aaronson and Alex Arkhipov. Bosonsampling is far from uniform. *Quantum Info. Comput.*, 14(15-16):1383–1423, November 2014.

[11] Leandro Aolita, Christian Gogolin, Martin Kliesch, and Jens Eisert. Reliable quantum certification for photonic quantum technologies. *arXiv preprint arXiv:1407.4817*, 2014.

[12] Nicolo Spagnolo, Chiara Vitelli, Marco Bentivegna, Daniel J Brod, Andrea Crespi, Fulvio Flamini, Sandro Giacomini, Giorgio Milani, Roberta Ramponi, Paolo Mataloni, et al. Experimental validation of photonic boson sampling. *Nature Photonics*, 8(8):615–620, 2014.

[13] I.Georgescu, S.Ashhab, and F.Nori. Quantum simulation. *Reviews of Modern Physics*, 86:153–185, Mar 2014.

[14] Stefanie Barz, Joseph F Fitzsimons, Elham Kashefi, and Philip Walther. Experimental verification of quantum computation. *Nature Physics*, 9(11):727–731, 2013.

[15] Matthew McKague. Interactive proofs for BQP via self-tested graph states, 2013. arXiv:1309.5675.

[16] Michal Hajdusek, Carlos A Perez-Delgado, and Joseph F Fitzsimons. Device-independent verifiable blind quantum computation. *arXiv preprint arXiv:1502.02563*, 2015.

[17] Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. Robustness and device independence of verifiable blind quantum computing. *arXiv preprint arXiv:1502.02571*, 2015.

[18] Masahito Hayashi and Tomoyuki Morimae. Verifiable measurement-only blind quantum computing with stabilizer testing. *arXiv preprint arXiv:1505.07535*, 2015.

[19] Vittorio Giovannetti, Lorenzo Maccone, Tomoyuki Morimae, and Terry G Rudolph. Efficient universal blind quantum computation. *Physical review letters*, 111(23):230501, 2013.

[20] Atul Mantri, Carlos A Perez-Delgado, and Joseph F Fitzsimons. Optimal blind quantum computation. *Physical review letters*, 111(23):230502, 2013.

[21] Carlos A Perez-Delgado and Joseph F Fitzsimons. Overcoming efficiency constraints on blind quantum computation. *arXiv preprint arXiv:1411.4777*, 2014.

[22] Robert Raussendorf, Jim Harrington, and Kovid Goyal. Topological fault-tolerance in cluster state quantum computation. *New Journal of Physics*, 9(6):199, 2007.

[23] R.Raussendorf and H.J.Briegel. A one-way quantum computer. *Physical Review Letters*, 86:5188, 2001.

[24] Vincent Danos, Elham Kashefi, and Prakash Panangaden. The measurement calculus. *Journal of the ACM (JACM)*, 54(2):8, 2007.

[25] Vincent Danos and Elham Kashefi. Determinism in the one-way model. *Physical Review A*, 74(5):052310, 2006.

[26] Mark Howard and Jiri Vala. Qudit versions of the qubit pi/8 gate. *Physical Review A*, 86(2):022316, 2012.

[27] Hussain Anwar. *Towards Fault-Tolerant Quantum Computation with Higher-Dimensional Systems*. PhD thesis, UCL (University College London), 2014.

[28] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[29] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 176–188. ACM, 1997.

[30] Howard Barnum, Claude Crepeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on*, pages 449–458. IEEE, 2002.

[31] Michael Ben-Or, Claude Crepeau, Daniel Gottesman, Avinatan Hassidim, and Adam Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *Foundations of Computer Science, 2006. FOCS'06. 47th Annual IEEE Symposium on*, pages 249–260. IEEE, 2006.

[32] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824, 1996.

[33] DLZhou, BZeng, ZXu, and CPSun. Quantum computation based on d-level cluster state. *Physical Review A*, 68(6):062303, 2003.

[34] William Hall. Cluster state quantum computation for many-level systems. *arXiv preprint quant-ph/0512130*, 2005.

A   Proof of Theorem 1

Single index notation is followed to enumerate the qubits participating in the graph where N is the total number of qubits and the last n' qubits are the encoded output qubits (system O'). Each measurement performed at Step 6d of the protocol is analysed into a unitary part and a Pauli Z measurement. Without loss of generality we can represent any dishonest behaviour of Bob at any step as applying the correct unitary operators and then an arbitrary unitary attack operator.

The output that Alice produces after she receives system O' from Bob and applies the decoding operators, averaged over all random parameters is:

$$\rho_{out} = Tr_{B,\mathcal{M},\Delta,D}(\sum_{\boldsymbol{b}} \sum_{\nu} p(\nu) C \mathcal{D}(|b_{N-n'}\rangle\langle b_{N-n'}|U_{N-n'}H_{N-n'}R_{N-n'}(\delta_{N-n'})(|\delta_{N-n'}\rangle\langle\delta_{N-n'}| \otimes \dots$$

$$|b_k\rangle\langle b_k|U_k H_k R_k(\delta_k)(|\delta_k\rangle\langle\delta_k| \otimes$$

$$\dots |b_1\rangle\langle b_1|U_1 H_1 R_1(\delta_1)(|\delta_1\rangle\langle\delta_1| \otimes E_G|M\rangle\langle M| \otimes |0\rangle\langle 0|^{\otimes B}E_G)R_1(\delta_1)^\dagger H_1 U_1^\dagger|b_1\rangle\langle b_1|\dots$$

$$)R_k(\delta_k)^\dagger H_k U_k^\dagger|b_k\rangle\langle b_k|\dots)R_{N-n'}(\delta_{N-n'})^\dagger H_{N-n'}U_{N-n'}^\dagger|b_{N-n'}\rangle\langle b_{N-n'}|)C^\dagger)(16)$$

where:

- $|M(\boldsymbol{\theta}, \boldsymbol{d}, \boldsymbol{t})\rangle$ is the state that Bob receives after Step 4 of the protocol (input, auxiliary qubits, dummy qubits).

- E_G is the global entangling operator that Bob applies at step 5 of the protocol.

- $\delta(\boldsymbol{\theta}, \boldsymbol{r}, \boldsymbol{b})$ is the vector of $\delta_i(\boldsymbol{\theta}, \boldsymbol{r}, \boldsymbol{b})$ which are measurement angles that Alice sends to Bob at iteration i of step 5 of the protocol .

- $R_i(\delta_i)$ is rotation of qubit i around z-axis by angle δ_i.

- H_i is a Hadamard gate applied on qubit i.

- U_i is the unitary attack of Bob with index i and applies on qubits $\geq i$, private Bob's system and all measurement angles.

- $\mathcal{D}$ is the map that Alice applies to decoding for the QECC used in the Fault Tolerant procedure.

- $C(\boldsymbol{r}, \boldsymbol{b})$ includes the Pauli correction $C_{O'}$ that Alice performs to the output system O' and the corrections to trap measurement results.

By commuting all measurement angles (trivially) and all attack unitary operators (by observing that they trivially commute with all measurements $\leq i$) and merge them into a new unitary U that applies on the whole of the system we get (see also Figure 2):
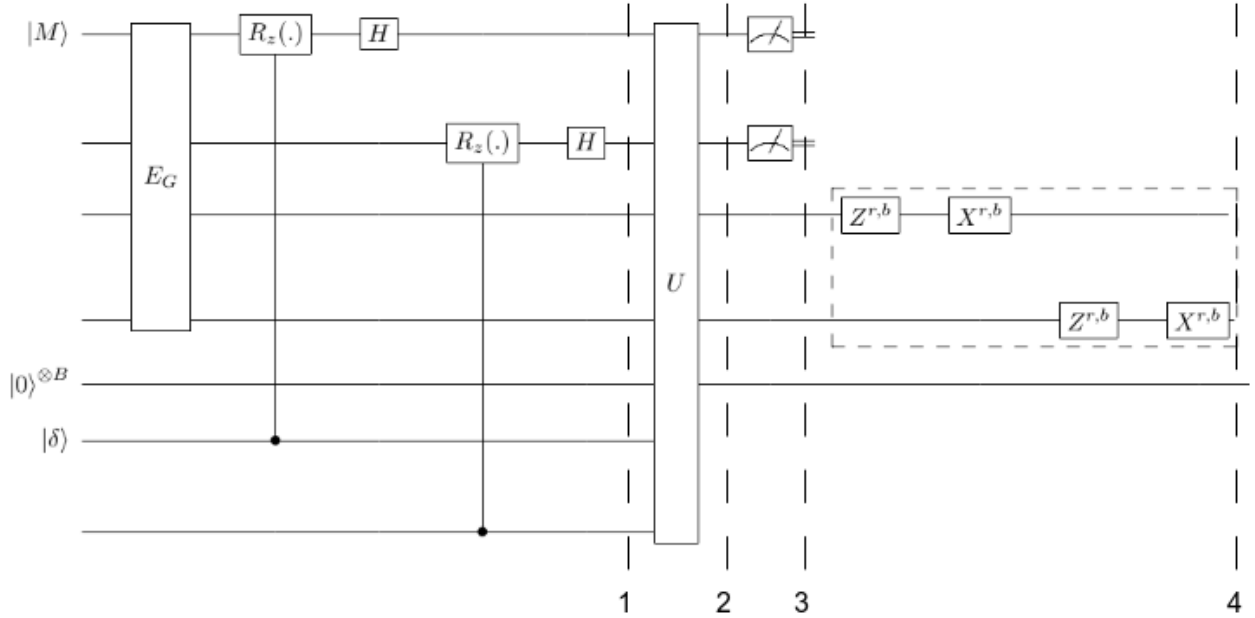

Figure 2: Analysis of attacks in the localising protocol. Part inside dashed box is applied by Alice.

$$\rho_{out} = Tr_{B,\mathcal{M},\Delta,D}(\sum_{\boldsymbol{b}} \sum_{\nu} p(\nu) C\mathcal{D}(|\boldsymbol{b}\rangle\langle\boldsymbol{b}| U (H_{N-n'} R_{N-n'}(.) \dots H_1 R_1(.) E_G($$

$$|M\rangle\langle M| \otimes |\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|) E_G R_1(.)^\dagger H_1 \dots R_{N-n'}(.)^\dagger H_{N-n'} \otimes |0\rangle\langle 0|^{\otimes B}) U^\dagger |\boldsymbol{b}\rangle\langle\boldsymbol{b}|) C^\dagger) \tag{17}$$

where U is a unitary attack operator that is chosen by Bob and applies on all graph qubits, private Bob's system and all measurement angles.

The trap system is not entangled with the rest when the honest computation is applied. We can separate the terms that apply on the trap (remember that the trap is placed among the measured qubits). Applying the entangling operators between the traps and their neighbours, which are always dummy qubits does not have any effect other than undoing the pre-rotation of the trap (for the case the dummy is selected to be $|1\rangle$). Applying $H_t R_t(\delta_t)$ on each trap, where $\delta_t = \theta_t + r_t \pi$, results in getting state $|r_t\rangle$.

Therefore, it holds that:

$$\mathcal{P}(|M\rangle\langle M| \otimes |\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|)\mathcal{P}^\dagger = \mathcal{P}'(|M'\rangle\langle M'| \otimes |\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|)\mathcal{P}'^\dagger \bigotimes_i |r_{t_i}\rangle\langle r_{t_i}| \tag{18}$$

where

- $\mathcal{P} = H_{N-n'}R_{N-n'}(.)\ldots H_{t_i}R_{t_i}(.)\ldots H_1 R_1(.)E_G$ is the correct unitary operation in Figure 2.

- $\mathcal{P}' = H_{N-n'}R_{N-n'}(.)\ldots H_1 R_1(.)E_G'$, which is produced from $\mathcal{P}$ by omitting all operations applied on traps (E_G' is produced from E_G by omitting all entangling operators between traps and their neighbours)

- $|M'\rangle$ is produced from $|M\rangle$ by omitting the trap qubits.

In the next step we express the output state with Bob's private system traced out and his attack decomposed to the Pauli basis. We use the following general property:

For any unitary U and n-qubit state ρ it holds that:

$$Tr_B(U(\rho \otimes |0\rangle\langle 0|^B)U^\dagger) = \sum_{k,u,u'} a_{k,u}a_{k,u'}^* P_u \rho P_{u'} \tag{19}$$

where

- $a_{k,u}$ are complex numbers, with $\sum_{k,u}|a_{k,u}|^2 = 1$.

- P_u (and $P_{u'}$) ranges over all general Pauli operators on n qubits.

Applying this property to the state in Equation 17, by tracing out system B, and at the same time applying Equation 18 to separate the traps we get the following form:

$$\rho_{out} = Tr_{\mathcal{M},\Delta,D}(\sum_{\boldsymbol{b}} \sum_{\nu} p(\nu) \sum_{k,u,v,u',v'} a_{k,u,v}a_{k,u',v'}^* C_{O'}\mathcal{D}(|\boldsymbol{b'}\rangle\langle\boldsymbol{b'}|P_{u|i:\forall j, i \neq t_j} \otimes P_v$$
$$(\mathcal{P}'(|M'\rangle\langle M'| \otimes |\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|)\mathcal{P}'^\dagger)P_{u'|i:\forall j, i \neq t_j} \otimes P_{v'}|\boldsymbol{b'}\rangle\langle\boldsymbol{b'}|)C_{O'}^\dagger$$
$$\bigotimes_i |b_{t_i} + r_{t_i}\rangle\langle b_{t_i}|P_{u|t_i}|r_{t_i}\rangle\langle r_{t_i}|P_{u'|t_i}|b_{t_i}\rangle\langle b_{t_i} + r_{t_i}|)) \tag{20}$$

where

- $a_{k,u,v}$ are complex numbers, with $\sum_{k,u,v}|a_{k,u,v}|^2 = 1$.

- P_u (and $P_{u'}$) ranges over all general Pauli operators and applies on the system that is trapified: all systems that are measured except those on the output gadget.

23

- P_v (and $P_{v'}$) ranges over all general Pauli operators and applies on the system that is not trapified: the whole of the gadget system O'' and the measurement angle system Δ.

- $P_{u|i}$ is the i-th Pauli element of P_u.

- $\boldsymbol{b}'$ is the vector that is generated from $\boldsymbol{b}$ by removing elements $\{b_{t_i}\}$.

In the next part of the proof the attack of Bob will be reduced to a mixture of Pauli operators, utilizing all random parameters except the random position of the trap to cancel the cross Pauli terms that are not the same.

By observing that $R_i(.)(|\psi\rangle \otimes |\delta_i\rangle)$ is equivalent mathematically to $R_i(\delta_i)|\psi\rangle \otimes |\delta_i\rangle$, since δ_i is a classical state we can rewrite

$$\mathcal{P}' = H_{N-n'}R_{N-n'}(\delta_{N-n'})\ldots H_1 R_1(\delta_1)E'_G =$$
$$H_{N-n'}R_{N-n'}(\phi'_{N-n'} + \theta_{N-n'} + r_{N-n'}\pi)\ldots H_1 R_1(\phi'_1 + \theta_1 + r_1\pi)E'_G =$$
$$H_{N-n'}R_{N-n'}(\phi'_{N-n'} + r_{N-n'}\pi)\ldots H_1 R_1(\phi'_1 + r_1\pi)E'_G R_{N-n'}(\theta_{N-n'})\ldots R_{N-n'}(\theta_i) =$$
$$\mathcal{P}'' R_{N-n'}(\theta_{N-n'})\ldots R_{N-n'}(\theta_i) \qquad (21)$$

Operations $R_{N-n'}(\theta_{N-n'})\ldots R_{N-n'}(\theta_i)$ when applied to states $|M\rangle$ (or not applying at all on dummies since θ is 0) they cancel the pre-rotation and the state is updated to a state which does not depend on $\boldsymbol{\theta}$, denoted by $|M'\rangle$.

Now that we have eliminated all dependences on $\boldsymbol{\theta}$ except for states $|\boldsymbol{\delta}\rangle$ we can sum over $\boldsymbol{\theta}$ to get for system Δ the state $P_{v|\Delta}\frac{1}{2^{|\Delta|}}IP_{v'|\Delta}$. For $P_{v|\Delta} = P_{v'|\Delta}$ this has trace 1 and for $P_{v|\Delta} \neq P_{v'|\Delta}$ it has trace 0, since all Pauli operators except identity are traceless. Therefore we can ignore the attack cross terms applied on the measurement angles system.

Next we consider the dummy qubits. Part of E'_G is applied between them and the computational qubits cancelling the pre-rotation of the latter when $d_i = 1$. The remaining entangling operators will be denoted by E''_G. Also for the rest of the operation applied on each dummy $i \in D$:

$$\sum_{d_i, r_i} H_i R_i(r_i\pi)|d_i\rangle\langle d_i|R_i(r_i\pi)H_i) = \frac{1}{2}I \qquad (22)$$

Again $Tr(P_{u|D}\frac{1}{2^{|D|}}IP_{u'|D})$ is 1 for $P_{u|D} = P_{u'|D}$ and 0 for $P_{u|D} \neq P_{u'|D}$ so we can ignore the cross terms of the attack applying on the dummy qubits. Let $|M''\rangle$ denote state $|M'\rangle$ without the traps and the dummy qubits.

The next step is an iteration over all qubits i of the graph state and using summation over each $\boldsymbol{r_i}$ to twirl each attack operator on qubit $f(i)$ respectively, where f is the flow function. We begin from qubit N and follow the reverse measuring order. We distinguish between tree types of qubits depending on their placement and we apply a different technique for each one:

- Qubit $i \in O'$: We extract stabilizer $Z_{f^{-1}(i)}^{r_{f^{-1}(i)}} X_i^{r_{f^{-1}(i)}}$ from graph $E''_G|M''\rangle$ (assuming that the final layer qubits are not entangled between them as it is the case in the graphs we consider in this work). This cancels dependence on $r_{f^{-1}(i)}$ on the operation applied on qubit $f^{-1}(i)$ and allows as to sum over $r_{f^{-1}(i)}$ (and r_i) to get property (using Lemma 3):

$$\sum_{r_{f^{-1}(i)}, r_i} Z_i^{b_{f^{-1}(j\sim i)} + r_{f^{-1}(j\sim i)}} X_i^{b_{f^{-1}(i)} + r_{f^{-1}(i)}} Z_i^{r_i} P_{v|i} X_i^{r_{f^{-1}(i)}} Z_i^{r_i} E''_G(|M^{(3)}\rangle\langle M^{(3)}|)$$

$$E''_G Z_i^{r_i} X_i^{r_{f^{-1}(i)}} P_{v'|i} Z_i^{r_i} X_i^{b_{f^{-1}(i)} + r_{f^{-1}(i)}} Z_i^{b_{f^{-1}(j\sim i)} + r_{f^{-1}(j\sim i)}} = 0 \text{ if } P_{v|i} \neq P_{v'|i} \qquad (23)$$

Note that for the terms that remain ($P_{v|i} = P_{v'|i}$) summing over $r_{f^{-1}(i)}, r_i$ eliminates all dependences from $r_{f^{-1}(i)}, r_i$ in the formula. Also note that $Z_i^{r_{f^{-1}(j\sim i)}}$ terms and all the b corrections remain.

- Qubit $i \notin O' \cup I$: We extract stabilizer $Z_{f^{-1}(i)}^{r_{f^{-1}(i)}} X_i^{r_{f^{-1}(i)}} Z_{j\sim i, j\neq f^{-1}(i)}^{r_{f^{-1}(i)}}$ from graph $E_G''|M^{(3)}\rangle$. This cancels dependence on $r_{f^{-1}(i)}$ on the operation applied on qubit $f^{-1}(i)$ and on operations applied on qubits $\{j \sim i, j \neq f^{-1}(i)\}$ (notice that attacks on qubits $\{j \sim i, j \neq f^{-1}(i)\}$ have already been twirled because we follow the opposite of flow). By summing the elements that still depend on $r_{f^{-1}(i)}$:

$$\sum_{r_{f^{-1}(i)}} \langle b_i | P_{u|i} H_i R_i(\phi_i' + r_i\pi)$$
$$X_i^{r_{f^{-1}(i)}} E_G''(|M^{(3)}\rangle\langle M^{(3)}|) E_G'' X_i^{r_{f^{-1}(i)}} R_i(\phi_i' + r_i\pi)^\dagger H_i P_{u'|i}|b_i\rangle \tag{24}$$

where $\phi_i' = (-1)^{b_{f^{-1}(i)} + r_{f^{-1}(i)}}\phi_i + (b_{f^{-1}(j\sim i, j\neq f(i))} + r_{f^{-1}(j\sim i, j\neq f(i))})\pi$.

This state is equal to

$$\sum_{r_{f^{-1}(i)}} \langle b_i | Z_i^{r_{f^{-1}}} P_{u|i} Z_i^{r_{f^{-1}}} H_i R_i(\phi_i'' + r_i\pi)$$
$$E_G''(|M^{(3)}\rangle\langle M^{(3)}|) E_G'' R_i(\phi_i'' + r_i\pi)^\dagger H_i Z_i^{r_{f^{-1}}} P_{u'|i} Z_i^{r_{f^{-1}}}|b_i\rangle \tag{25}$$

where $\phi_i'' = (-1)^{b_{f^{-1}(i)}}\phi_i + (b_{f^{-1}(j\sim i, j\neq f(i))} + r_{f^{-1}(j\sim i, j\neq f(i))})\pi$.

To get the above state we used also the fact that we can extract a random $Z_i^{r_{f^{-1}}}$ from both $\langle b_i|$ and $|b_i\rangle$, without affecting the state.

To apply Lemma 3 we also need the random X elements. These are acquired by extracting stabilizer $Z_i^{r_i'} X_{f(i)}^{r_i'} Z_{j\sim f(i), j\neq i}^{r_i'}$ from graph $E_G''|M^{(3)}\rangle$ and also changing variable $b_i^\diamond \leftarrow b_i + r_i'$ for $r_i' \leftarrow_R \{0,1\}$. The new terms cancel everywhere except at qubit i so that we get:

$$\sum_{r_{f^{-1}(i)}, r_i'} \langle b_i^\diamond | X^{r_i'} Z_i^{r_{f^{-1}}} P_{u|i} Z_i^{r_{f^{-1}}} X^{r_i'} H_i R_i(\phi_i'' + r_i\pi) E_G''(|M^{(3)}\rangle\langle M^{(3)}|) E_G''$$
$$R_i(\phi_i'' + r_i\pi)^\dagger H_i X^{r_i'} Z_i^{r_{f^{-1}}} P_{u'|i} Z_i^{r_{f^{-1}}} X^{r_i'}|b_i^\diamond\rangle = 0 \text{ if } P_{u|i} \neq P_{u'|i} \tag{26}$$

- Qubit $i \in I$: We use property $XR(\phi)|+\rangle = e^{i\phi}R(-\phi)|+\rangle$ We extract stabilizer $X_1^{z_0} Z_{f(i)}^{z_0}$ from graph $E_G''|M^{(3)}\rangle$ (graphs we use have the property that inputs i are only entangled with $f(i)$), where $z_0 \leftarrow \{0,1\}$. Also extract a random Z^{z_0} from $\langle b_i|$ and from $|b_i\rangle$ and employing the same trick for generating the X elements that we did in the previous step and then applying Lemma 3 gives us:

$$\sum_{x_0, z_0} \langle b_i | X^{x_0} Z^{z_0} P_{u|i} Z^{z_0} X^{x_0} H_i R_i(\phi_i + r_i\pi)$$
$$E_G''(|M^{(3)}\rangle\langle M^{(3)}|) E_G'' R_i(\phi_i + r_i\pi)^\dagger H_i X^{x_0} Z^{z_0} P_{u'|i} Z^{z_0} X^{x_0}|b_i\rangle = 0 \text{ if } P_{u|i} \neq P_{u'|i} \tag{27}$$

Finally we consider the trap qubits t_i:

$$\sum_{r_{t_i}, b_{t_i}} |b_{t_i} + r_{t_i}\rangle\langle b_{t_i}|P_{u|t_i}|r_{t_i}\rangle\langle r_{t_i}|P_{u'|t_i}|b_{t_i}\rangle\langle b_{t_i} + r_{t_i}| \tag{28}$$

By changing variable $b_{t_i}^\diamond \leftarrow b_{t_i} + r_{t_i}$

$$\sum_{r_{t_i}, b_{t_i}^\diamond} |b_{t_i}^\diamond\rangle\langle b_{t_i}^\diamond|X^{r_{t_i}}P_{u|t_i}X^{r_{t_i}}|0\rangle\langle 0|X^{r_{t_i}}P_{u'|t_i}X^{r_{t_i}}|b_{t_i}^\diamond\rangle\langle b_{t_i}^\diamond|$$

$$= \sum_{r_{t_i}, r'_{t_1}, b_{t_i}^\diamond} |b_{t_i}^\diamond\rangle\langle b_{t_i}^\diamond|Z^{r'_{t_i}}X^{r_{t_i}}P_{u|t_i}X^{r_{t_i}}Z^{r'_{t_i}}|0\rangle\langle 0|Z^{r'_{t_i}}X^{r_{t_i}}P_{u'|t_i}X^{r_{t_i}}Z^{r'_{t_i}}|b_{t_i}^\diamond\rangle\langle b_{t_i}^\diamond|$$

$$= 0 \text{ if } P_{u|t_i} \neq P_{u'|t_i} \tag{29}$$

Thus we have zeroed all terms where $u \neq u$ and $v \neq v$ which gives:

$$\rho_{out} = \sum_{\boldsymbol{b}} \sum_{\boldsymbol{t}} p(\boldsymbol{t}) \sum_{k,u,v} |a_{k,u,v}|^2 C'_{O'} \mathcal{D}(\langle \boldsymbol{b}'|P_{u|i:\forall j, i \neq t_j} \otimes P_{v|O''}$$

$$(\mathcal{P}^{(3)}(|M^{(3)}\rangle\langle M^{(3)}|)\mathcal{P}^{(3)\dagger})P_{u|i:\forall j, i \neq t_j} \otimes P_{v|O''}|\boldsymbol{b}'\rangle)C'^{\dagger}_{O'} \bigotimes_i P_{u|t_i}|0\rangle\langle 0|P_{u|t_i} \tag{30}$$

where

- $|M^{(3)}\rangle$ is the tensor product of $|+\rangle$ for all qubits of system $\mathcal{M} \times O'$.

- $\mathcal{P}^{(3)}$ is the unitary that contains E'_G for $\mathcal{M} \times O'$ and $H_i R_i((-1)^{b_{f^{-1}(i)}}\phi_i + b_{f^{-1}(j \sim i, j \neq f(i))}\pi)$ operators for all qubits of system $\mathcal{M}$.

- C' are the remaining Pauli corrections on the output system O' (after eliminating the r's) and depend only on $\boldsymbol{b}$.

We split the sum over the attack operators P_u (applying on the trapified system) in Equation 30 into the operators which are perfectly corrected by the QECC used in the FK protocol and the operators which are not corrected but have a significant footprint to be caught by the trapification procedure with high probability.

Specifically, restricting the summation in the state of Equation 30 to $u \in \mathcal{S}_1$ where $\mathcal{S}_1$ is the set of general Pauli operators that contain $\leq d$ elements which have a Pauli X component (where d is the number of correctable errors of the code), we have state:

$$\sigma_1 = \sum_{\boldsymbol{b}} \sum_{\boldsymbol{t}} p(\boldsymbol{t}) \sum_{k, u \in \mathcal{S}_1, v} |a_{k,u,v}|^2 C'_{O'} \mathcal{D}\langle \boldsymbol{b}'|P_{u|i:\forall j, i \neq t_j} \otimes P_{v|O''}$$

$$(\mathcal{P}^{(3)}(|M^{(3)}\rangle\langle M^{(3)}|)\mathcal{P}^{(3)\dagger})P_{u|i:\forall j, i \neq t_j} \otimes P_{v|O''}|\boldsymbol{b}'\rangle)C'^{\dagger}_{O'} \bigotimes_i P_{u|t_i}|0\rangle\langle 0|P_{u|t_i} \tag{31}$$

Let us separate the terms of the Pauli attack $P_{v|O''}$ on the gadget system to those applying on the measured qubits, say P_{v_1}, and those who apply on the output system O' qubits, say P_{v_2}.

The X-component of attack P_{v_1}, denoted by P'_{v_1}, can be replaced by a P'_{v_1} attack on output system O' (since it affects the X corrections of the output) and the Z-component of attack P_{v_1} does not have any effect on the state. Note that if we wanted to reduce attacks of previous measurement layers to attacks on the output these attacks would have a correlation with the output, but in the case of the last measurement layer this does not happen.

Commuting the output Pauli attacks $P'_{v_1}P_{v_2}$ with the decoding operator $\mathcal{D}$ updates them to a different Pauli operator $P''_{v_1}P'_{v_2}$:

$$= \sum_{\boldsymbol{b}} \sum_{\boldsymbol{t}} p(\boldsymbol{t}) \sum_{k,u \in \mathcal{S}_1, v} |a_{k,u,v}|^2 C'_{O'} \langle \boldsymbol{b}'| P_{u|i:\forall j, i \neq t_j} \otimes P''_{v_1} P'_{v_2} \mathcal{D}$$
$$(\mathcal{P}^{(3)}(|M^{(3)}\rangle\langle M^{(3)}|)\mathcal{P}^{(3)\dagger}) P_{u|i:\forall j, i \neq t_j} \otimes \mathcal{D}^\dagger P'_{v_2} P''_{v_1} |\boldsymbol{b}'\rangle) C'^\dagger_{O'} \bigotimes_i P_{u|t_i} |0\rangle\langle 0| P_{u|t_i} \tag{32}$$

Since $P_u \in \mathcal{S}_1$ attack $P_{u|i:\forall j, i \neq t_j}$ and the QECC perfectly corrects d errors, the attack will not have any effect on the correct (quantum one-time-padded) outcome after applying the measurements and decoding.

$$= \sum_{\boldsymbol{b}} \sum_{\boldsymbol{t}} p(\boldsymbol{t}) \sum_{k,u \in \mathcal{S}_1, v} |a_{k,u,v}|^2 C'_{O'} P''_{v_1} P'_{v_2} (C'_O |\psi_c\rangle\langle \psi_c| C'_{O'}) P'_{v_2} P''_{v_1} C'^\dagger_O) \bigotimes_i P_{u|t_i} |0\rangle\langle 0| P_{u|t_i} \tag{33}$$

We can further eliminate $C'_{O'}$ by commuting through output attacks.

By separating the terms that leave all traps untouched and the rest and tracing out $O' \setminus O$ we get:

$$\sigma_1 = \sum_i p'_i P_i |\psi_c\rangle\langle \psi_c|) P_i \otimes |ACC\rangle\langle ACC| + \sum_j p''_j P_j |\psi_c\rangle\langle \psi_c| P_j \otimes |REJ\rangle\langle REJ| \tag{34}$$

where

- P_i (P_j) range over all general Pauli operators on the output system O.

- p'_i, p''_i are probabilities with $\sum_i (p'_i + p''_i) = \sum_{k,u \in \mathcal{S}_1, v} |a_{k,u,v}|^2$.

- $|ACC\rangle\langle ACC|$ is the state where all trap qubits are $|0\rangle\langle 0|$ and $|REJ\rangle\langle REJ|$ denotes any state that at least one trap is $|1\rangle\langle 1|$.

- $|\psi_c\rangle\langle \psi_c|$ is the correct state for the output system O, which crucially is placed on a fixed position which does not depend on the selection of the trap positions ($\boldsymbol{t}$) (since the position of O' was also fixed due to the structure of the gadget and the decoding circuit is fixed).

We examine the rest of the terms of the summation in the state in Equation 30 (where $u \in \mathcal{S}_2$ means that P_u contains $> d$ Pauli elements with a Pauli X component).

Let $P_\perp$ be the projection to the orthogonal space to the correct output state:

$$P_\perp = I - |\psi_c\rangle\langle \psi_c| \tag{35}$$

We calculate the 'bad' probability p_{bad} the state collapses to the 'incorrect' subspace and no trap is activated.

$$p_{\text{bad}} = Tr(\sum_{\boldsymbol{t}} p(\boldsymbol{t}) P_\perp \bigotimes_i |0\rangle_{t_i}\langle 0|_{t_i} (\sum_{\boldsymbol{b}} \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 C'_{O'}\mathcal{D}(\langle\boldsymbol{b}'|P_{u|i:\forall j, i\neq t_j} \otimes P_{v|O''}$$

$$(\mathcal{P}^{(3)}(|M^{(3)}\rangle\langle M^{(3)}|)\mathcal{P}^{(3)\dagger})P_{u|i:\forall j, i\neq t_j} \otimes P_{v|O''}|\boldsymbol{b}'\rangle)C'^\dagger_{O'} \bigotimes_i P_{u|t_i}|0\rangle_{t_i}\langle 0|_{t_i} P_{u|t_i}) \tag{36}$$

Tracing out $P_\perp(\sum_{\boldsymbol{b}} C'_{O'}\mathcal{D}(\langle\boldsymbol{b}'|P_{u|i:\forall j, i\neq t_j}\otimes P_{v|O''}(\mathcal{P}^{(3)}(|M^{(3)}\rangle\langle M^{(3)}|)\mathcal{P}^{(3)\dagger})P_{u|i:\forall j, i\neq t_j}\otimes P_{v|O''}|\boldsymbol{b}'\rangle)C'^\dagger_{O'}$:

$$\leq Tr(\sum_{\boldsymbol{t}} p(\boldsymbol{t})|0\rangle_{t_i}\langle 0|_{t_i} \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 \bigotimes_i P_{u|t_i}|0\rangle_{t_i}\langle 0|_{t_i} P_{u|t_i}) \tag{37}$$

Or:

$$= \prod_i \sum_{t_i} p(t_i) \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 |\langle 0|_{t_i} P_{u|t_i}|0\rangle_{t_i}|^2 \tag{38}$$

We can divide the measured positions into $|\boldsymbol{t}|$ subsets S_γ where each trap position t_γ is chosen uniformly at random between the $|S_{t_\gamma}| = 1/c'$ positions (revealing this information can only deteriorate the security, so the bound will be true also for the previous case):

$$= \prod_{\gamma=1}^{|\boldsymbol{t}|} \sum_{t_\gamma\in S_\gamma} p(t_\gamma) \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 |\langle 0|_{t_\gamma} P_{u|t_\gamma}|0\rangle_{t_\gamma}|^2 \tag{39}$$

Denoting by $w_{u,\gamma}$ the number of positions such that $P_{u|t_\gamma}$ (over all $1/c'$ values that the particular t_γ can take) is either Pauli X or Y:

$$= \prod_{\gamma=1}^{|\boldsymbol{t}|} c' \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 (\frac{1}{c'} - w_{u,\gamma})$$

$$\leq \prod_{\gamma=1}^{|\boldsymbol{t}|} \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 (1 - c')^{w_{u,\gamma}} \tag{40}$$

where the last inequality comes from the fact that $w_{u,\gamma}$ is non-negative integer.

$$= \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 (1 - c')^{\sum_{\gamma=1}^{|\boldsymbol{t}|} w_{u,\gamma}}$$

$$\leq \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 (1 - c')^d \tag{41}$$

where the last inequality comes from the fact that since $u \in \mathcal{S}_2$, it follows that the total footprint $\sum_{\gamma=1}^{|\boldsymbol{t}|} w_{u,\gamma}$ of attack P_u is $> d$.

Therefore state can be written as:

$$\sigma_2 \approx_{\sqrt{(1-c')^d}} p(\sum_{k,u \in \mathcal{S}_2, v} |a_{k,u,v}|^2)|\psi_c\rangle\langle\psi_c| \otimes |ACC\rangle\langle ACC|$$

$$+ (1-p)(\sum_{k,u \in \mathcal{S}_2, v} |a_{k,u,v}|^2)\rho \otimes |REJ\rangle\langle REJ| \tag{42}$$

for some probability p and density matrix ρ. Or,

$$\sigma_2 \approx_{\sqrt{(1-c')^d}} p_1|\psi_c\rangle\langle\psi_c| \otimes |ACC\rangle\langle ACC| + p_2\rho \otimes |REJ\rangle\langle REJ| \tag{43}$$

where

- $p_1 + p_2 = \sum_{k,u \in \mathcal{S}_2, v} |a_{k,u,v}|^2$

- ρ is a density matrix.

Summing the terms σ_1 and σ_2, Theorem 1 is satisfied with $\epsilon = \sqrt{(1-c')^d}$.

B   Proof of Theorem 2

For any run of Protocol 2, for any choice of Alice's input computation (therefore for any choice of sign keys used in the ABE protocol phase), the output that Alice has at the end of the protocol before applying the ABE detection procedure, averaged over all random parameters except the sign key, is:

$$\rho_{out} = Tr_{B,\mathcal{M},\Delta,D,\mathcal{L}}(\sum_{\boldsymbol{b},\widetilde{\boldsymbol{b}}} \sum_{\nu} p(\nu)C''(|\boldsymbol{b}\rangle\langle\boldsymbol{b}| \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|U\mathcal{C}\mathcal{D}(F_{N-n'}R_{N-n'}(.)\ldots F_1R_1(.)E_G($$

$$|M\rangle\langle M| \otimes |\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|)E_G R_1(.)^\dagger F_1^\dagger \ldots R_{N-n'}(.)^\dagger F_{N-n'}^\dagger \otimes |0\rangle\langle0|^{\otimes B} \otimes |\widetilde{\boldsymbol{r}}\rangle\langle\widetilde{\boldsymbol{r}}|)\mathcal{D}^\dagger\mathcal{C}^\dagger U^\dagger|\boldsymbol{b}\rangle\langle\boldsymbol{b}| \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|)C'')(44)$$

where:

- $R_i(\delta_i)$ corresponds the diagonal generalized Clifford operation $T^{c_i}S^{b_i}Z^{a_i}$ controlled by the state of vector δ_i.

- F_i is the Fourier gate applied on qubit i.

- $\mathcal{D}$ is the Clifford unitary used to decode the output O' of the FK protocol phase which is encoded by the QECC used by the FK protocol. The decoding is applied by Bob in this case and the decoded state is contained in subsystem O of O'.

- $|\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|$ implement the measurements for the Toffoli gates at the ABE protocol phase and apply on some of the qubits of system O (see Figure 3).

- $\widetilde{\boldsymbol{r}}(\boldsymbol{r}, \widetilde{\boldsymbol{b}})$ is the classical bit string (system $\mathcal{L}$) that Alice sends to Bob for the corrections of the Toffoli part of the ABE protocol.

- $\mathcal{C}(\widetilde{\boldsymbol{r}})$ is the Clifford part of the ABE protocol phase that implements the public polynomial-QECC logical circuit on system O.

- $C''(\boldsymbol{r}, \boldsymbol{b})$ contains the Pauli correction $C''_{O'}$ that Alice performs to the final returned system, that takes into account the updates of the keys due to the application of circuits $\mathcal{D}$ and $\mathcal{C}$. C'' also contains the corrections to trap measurement results.

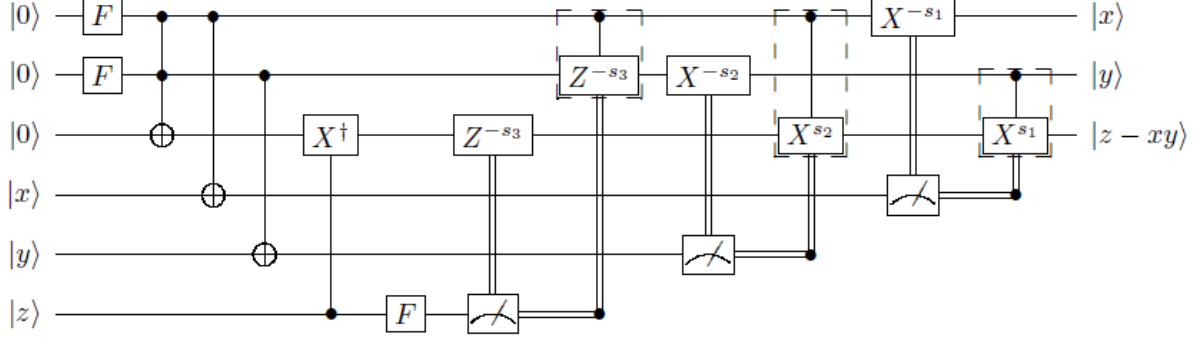- U represents global Bob's attack that in this case applies also to system $\mathcal{L}$.

Figure 3: Implementation of Toffoli gate with Toffoli state, Clifford operators and Pauli Z measurements. The corrections (which have to be performed by Bob depending on his communication with Alice) are the Clifford operators in the dashed boxes.

Alice's output can be rewritten, by decomposing the attack to the Pauli basis, tracing out system B and applying the honest computation on system T to separate it, as:

$$\rho_{out} = Tr_{\mathcal{M},\Delta,D,\mathcal{L}}(\sum_{\boldsymbol{b},\widetilde{\boldsymbol{b}}}\sum_{\nu}p(\nu)\sum_{k,u,v,u',v'}a_{k,u,v}a^*_{k,u',v'}C''_{O'}(|\boldsymbol{b}'\rangle\langle\boldsymbol{b}'|\otimes|\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|P_{u|i:\forall j,i\neq t_j}\otimes P_v$$

$$\mathcal{C}\mathcal{D}(\mathcal{P}'(|M'\rangle\langle M'|\otimes|\boldsymbol{\delta}\rangle\langle\boldsymbol{\delta}|)\mathcal{P}'^\dagger)\mathcal{D}^\dagger\mathcal{C}^\dagger P_{u'|i:\forall j,i\neq t_j}\otimes P_{v'}|\boldsymbol{b}'\rangle\langle\boldsymbol{b}'|\otimes|\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|)C''^\dagger_{O'}$$

$$\bigotimes_i|b_{t_i}+r_{t_i}\rangle\langle b_{t_i}|P_{u|t_i}|r_{t_i}\rangle\langle r_{t_i}|P_{u'|t_i}|b_{t_i}\rangle\langle b_{t_i}+r_{t_i}|)) \qquad (45)$$

where

- $a_{k,u,v}$ are complex numbers, with $\sum_{k,u,v}|a_{k,u,v}|^2 = 1$.

- P_u (and $P_{u'}$) ranges over all general d-level Pauli operators and applies on the system that is trapified.

- P_v (and $P_{v'}$) ranges over all general d-level Pauli operators and applies on the system that is not trapified: $O'' \times \Delta \times \mathcal{L}$.

- $P_{u|i}$ is the i-th generalized Pauli element of P_u (similarly for P_v).

- $\boldsymbol{b}'$ is the vector that is generated from $\boldsymbol{b}$ by removing elements $\{b_{t_i}\}$.

We notice that we can extract a random logical Pauli $Z^{r'_1}\otimes Z^{r'_2}\otimes Z^{r'_3}$ from state $|000\rangle$ that is used to prepare the Toffoli gate (Figure 3) and notice that the dependences on (r'_1, r'_2, r'_3) cancel in all systems except system $\mathcal{L}$. Then, summing over (r'_1, r'_2, r'_3) gives the maximally mixed state for

system $\mathcal{L}$ and thus taking the trace of it cancels all cross terms of the corresponding attack. The rest of the arguments follow the corresponding part of the proof of Theorem 1.

Therefore state ρ_{out} can be rewritten to eliminate all Pauli cross terms from the attack of Bob that are different.

$$\rho_{out} = \sum_{b,\widetilde{b}} \sum_{t} p(\boldsymbol{t}) \sum_{k,u,v} |a_{k,u,v}|^2 C_{O'}^{(3)} (\langle \boldsymbol{b'}| \otimes |\widetilde{\boldsymbol{b}}\rangle \langle \widetilde{\boldsymbol{b}}| P_{u|i:\forall j, i \neq t_j} \otimes P_{v|O''}$$

$$(\mathcal{C}\mathcal{D}(\mathcal{P}^{(3)}(|M^{(3)}\rangle\langle M^{(3)}|)\mathcal{P}^{(3)\dagger})\mathcal{D}^\dagger \mathcal{C}^\dagger) P_{u|i:\forall j, i \neq t_j} \otimes P_{v|O''} |\boldsymbol{b'}\rangle \otimes |\widetilde{\boldsymbol{b}}\rangle \langle \widetilde{\boldsymbol{b}}|) C_{O'}^{(3)\dagger} \bigotimes_{i} P_{u|t_i} |0\rangle\langle 0| P_{u|t_i} \quad (46)$$

where

- $|M^{(3)}\rangle$ is the tensor product of $|+_0\rangle$ for all qudits of system $\mathcal{M} \times O'$.

- $\mathcal{P}^{(3)}$ is the unitary that contains E'_G for $\mathcal{M} \times O'$ and $F_i R_i(\phi'_i(b_{f^{-1}(i)}, b_{f^{-1}}(j \sim i, j \neq f(i)))$ operators for all qudits of system $\mathcal{M}$.

- $C_{O'}^{(3)}$ are the corrections on the output of the ABE protocol phase (after eliminating the r's) and depend on $\boldsymbol{b'}$ and $\widetilde{\boldsymbol{b}}$.

Restricting the summation to $u \in \mathcal{S}_1$ where $\mathcal{S}_1$ is the set of general d-level Pauli operators that contain $\leq d_1$ elements which have a generalized Pauli X component (where d_1 is the number of correctable errors of the code) and applying the same steps as in the corresponding part of the proof of Theorem 1, the state becomes:

$$\sigma_1 = \sum_{b} \sum_{t} p(\boldsymbol{t}) \sum_{k,u \in \mathcal{S}_1, v} |a_{k,u,v}|^2 C_{O'}^{(3)} P''_{v_1} P'_{v_2} (C_{O'}^{(3)} |\psi'_c\rangle\langle\psi'_c| C_{O'}^{(3)}) P'_{v_2} P''_{v_1} C_{O'}^{(3)} \bigotimes_{i} P_{u|t_i} |0\rangle\langle 0| P_{u|t_i} \quad (47)$$

The fact that the graph is partitioned into sub-graphs, to encode the different logical states to be used in the ABE protocol phase does not change the above statement because a global attack with footprint $\leq d_1$ will necessarily have footprint $\leq d_1$ in each sub-graph. We can also eliminate $C_{O'}^{(3)}$ by commuting with the Pauli attack operators.

By separating the terms that leave all traps untouched and the rest we get:

$$\sigma_1 = \sum_{i} p'_i P_i |\psi'_c\rangle\langle\psi'_c| P_i \otimes |ACC_1\rangle\langle ACC_1| + \sum_{j} p''_j P_j |\psi'_c\rangle\langle\psi'_c| P_j \otimes |REJ_1\rangle\langle REJ_1| \quad (48)$$

where

- P_i (P_j) range over all general d-level Pauli operators on the final returned system.

- p'_i , p''_i are probabilities with $\sum_i (p'_i + p''_i) = \sum_{k,u \in \mathcal{S}_1, v} |a_{k,u,v}|^2$.

- $|ACC_1\rangle\langle ACC_1|$ is the state where all trap qubits are $|0\rangle\langle 0|$ and $|REJ_1\rangle\langle REJ_1|$ denotes any state that at least one trap is $|1\rangle\langle 1|$.

- $|\psi'_c\rangle\langle\psi'_c|$ is the state, encoded by the signed polynomial QECC, after the correct computation of the ABE protocol phase is performed and undoing the Pauli key.

The rest of the terms of the summation in the state ρ_{out} ($u \in \mathcal{S}_2$) are considered. Let $P_\perp$ be the projection to the orthogonal space to the correct output state:

$$P_\perp = I - |\psi'_c\rangle\langle\psi'_c| \tag{49}$$

We calculate the 'bad' probability p_{bad} the state collapses to the 'incorrect' subspace and no trap is activated.

$$p_{\text{bad}} = Tr(\sum_{\boldsymbol{b},\widetilde{\boldsymbol{b}}}\sum_{\boldsymbol{t}} p(\boldsymbol{t})P_\perp \bigotimes_i |0\rangle_{t_i}\langle0|_{t_i} \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 C_{O'}^{(3)}(\langle\boldsymbol{b}'| \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|P_{u|i:\forall j, i\neq t_j} \otimes P_{v|O''}$$

$$(\mathcal{C}\mathcal{D}(\mathcal{P}^{(3)}(|M^{(3)}\rangle\langle M^{(3)}|)\mathcal{P}^{(3)\dagger})\mathcal{D}^\dagger\mathcal{C}^\dagger)P_{u|i:\forall j, i\neq t_j} \otimes P_{v|O''}|\boldsymbol{b}'\rangle \otimes |\widetilde{\boldsymbol{b}}\rangle\langle\widetilde{\boldsymbol{b}}|)C_{O'}^{(3)\dagger}\bigotimes_i P_{u|t_i}|0\rangle\langle0|P_{u|t_i}) \tag{50}$$

Tracing out everything except the trap system:

$$\leq Tr(\sum_{\boldsymbol{t}} p(\boldsymbol{t})|0\rangle_{t_i}\langle0|_{t_i} \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2 \bigotimes_i P_{u|t_i}|0\rangle_{t_i}\langle0|_{t_i}P_{u|t_i}) \tag{51}$$

The rest is the same to the corresponding part in the proof of Theorem 1 giving the final state:

$$\sigma_2 \approx_{\sqrt{(1-c')^{d_1}}} p_1|\psi'_c\rangle\langle\psi'_c| \otimes |ACC_1\rangle\langle ACC_1| + p_2\rho \otimes |REJ_1\rangle\langle REJ_1| \tag{52}$$

where $p_1 + p_2 = \sum_{k,u\in\mathcal{S}_2,v} |a_{k,u,v}|^2$ and ρ is a density matrix.

By summing the states σ_1 and σ_2 and by contractiveness of the ABE protocol detection procedure that Alice applies to check if the state is in the valid space of the signed polynomial QECC, Theorem 2 is satisfied with $\epsilon_1 = \sqrt{(1-c')^{d_1}}$ and $\epsilon_2 = (1/2)^{d_2}$.